BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems

Volume 4 • Issue 1 • April 2022 ISSN 2661-3204 (Online)

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 Issue 1 • April 2022 • ISSN 2661-3204 (Online)

Journal of Electronic & Information Systems

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 | Issue 1 | April 2022 | Page1-32
Journal of Electronic & Information Systems

Contents

Articles

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems
https://ojs.bilpublishing.com/index.php/jeis

ARTICLE

Collective Signature Schemes Problem of Finding Roots Modulo

Hailyie Tekleselassie[1,2*]

1. School of Informatics, Wolaita Sodo University, Wolaita sodo, Ethiopia
2. Department of Information Systems, addis ababa, Ethiopia

ARTICLE INFO

Article history
Received: 15 December 2021
Accepted: 7 March 2022
Published Online: 21 March 2022

Keywords:
Computing roots
Finding roots modulo
Collective signature
Signing collective
Signing group

ABSTRACT

Digital signature schemes in general and representative collective digital signature schemes, in particular, are often built based on the difficulty of the discrete logarithm problem on the finite field, of the discrete logarithm problem of the elliptic curve, of the problem of factor analysis, of the problem of finding the roots modulo of large primes or a combination of the difficult problems mentioned above. In this paper, we use the new difficult problem, which is to find the w^{th} root in the finite ground field to build representative collective signature schemes, but the chosen modulo has a special structure distinct $p = Nt_0t_1t_2 + 1$, where N is an even number and t_0, t_1, t_2 are prime numbers of equal magnitude, about $80\ bits$. The characteristics of the proposed scheme are: i) The private key of each signer consists of 2 components (K_1, K_2), randomly selected, but the public key has only one component (Y) calculated by the formula $Y = K_1^{w1}K_2^{w2}$; and t_0t_2; and ii) The generated signature consists of a set of 3 components (e, S_1, S_2). We use the technique of hiding the signer's public key Y, which is the coefficient λ generated by the group manager, in the process of forming the group signature and representative collective signature to enhance the privacy of all members of the signing collective.

1. Introduction

Digital signatures [1] play an important role in authentication systems in today's cyberspace. Other network security services such as ensuring the integrity of information transmitted on the network, preventing the disclaimer of responsibility of a communication partner, etc also need the support of digital signatures [2]. It can be said that digital signatures contribute to making cyberspace safer and more reliable. Therefore, digital signatures and digital signature schemes are increasingly interested in research by cryptographic scientists.

Digital signature is not only used to authenticate a single signer, but it can also support authentication for a collective, or a group, consisting of many different members. These people work together to create a single signature that represents an entire signing group or a group of signatures. Currently, there are many forms of digital signatures and digital signature schemes, in order to meet

*Corresponding Author:
Hailyie Tekleselassie,
School of Informatics, Wolaita Sodo University, Wolaita sodo, Ethiopia; Department of Information Systems, addis ababa, Ethiopia;
Email: hailyie.tekleselase@wsu.edu.et

DOI: https://doi.org/10.30564/jeisr.v4i1.4220

many different authentication models, which have been researched, published and applied in practice such as: Single digital signatures, group digital signatures [3-6], collective digital signatures [7-9], blind digital signatures [10,11], blind collective digital signatures [12], representative collective signatures [13]. The types of signatures generated by a set of signers are often referred to as multi-signatures [14,15].

The group signature is a signature representing a signing group, the signature formation is controlled by the group manager, the group manager's public key is used to verify the validity of the group signature of the signing group. The collective signature is a signature that represents a signing collective, signature formation is done by all members of the collective, the public key is used to check the validity of the collective signature is formed the public key of all members who participated in creating the signature. A collective signature on document M is considered valid when it is formed by the participation of all members of that signing collective. Representative collective signature is a new form of collective signature. We rely on the advantages of the group signature scheme and the collective signature scheme to develop the representative collective signature scheme.

A representative collective signature [8] is formed from a signing collective consisting of: i) Many groups of members, called signing groups, each group is represented by a group manager; and ii) A number of single individuals, known as individual signers, who do not belong to any group, but are functionally equivalent to the group leaders in this collective. Thus, a single representative collective signature can authenticate all members of a multi-level functional collective who are the creators of this representative collective signature. There are three difficult problems commonly used to build digital signature schemes, which are: i) The problem of parsing a composite number into prime factors [16]; ii) Discrete logarithm problem on prime finite field [17]; and iii) Discrete logarithm problem on Elliptic curves [18,19].

The problem of finding modulo roots in finite fields is a new difficult problem, introduced by Nikolay A. Moldovan. According to the author, the problem of finding the prime modulo root (with a prime modulo being a large prime p, has the special structure $p = Nk^2 + 1$, $|p| \geq 1024$, N being an even number and k is prime, $|k| \geq 160$) is a hard problem, the estimated difficulty is $O(\sqrt{k})$. Digital signature schemes built on this difficult problem can achieve security level 2^{80}, however, the time cost of signature generation and signature checking is an issue that needs to be considered for improvement. According to Nikolay A. Moldovyan, this time cost limitation can be overcome if the difficult problem of finding prime modulo roots is considered in a finite field, with p having the following structure $p = Nt_0t_1t_2 + 1$, where N is an even number; t_0, t_1, are prime numbers of the same magnitude as 80 bits.

The key pair of the signer in the case of $p = NK^2 + 1$ is (x, y), the private key is chosen at random, the public key is calculated by the formula $y = x^k \bmod p$. But in case is (K_1, K_2) and Y). That is, the private key consists of two components and K_2, the public key is still one component Y. This is the difference of the signature schemes described in this paper.

In this paper, we use the difficult problem of finding roots modulo in a finite ground field, with a prime modulo with the structure and a single signature scheme described by Nikolay A. Moldovyan to build the collective signature scheme and the group signature scheme. From these two basic schemes, we propose and build two types of representative collective signature scheme, proposed by us: i) The collective signature scheme for many signing groups (the RCS.01-3 scheme); and ii) The collective signature scheme for many signing groups and many individual signers (the RCS.02-3 scheme). These schemes fully inherit the security advantages of the newly created difficult problem and the attack resistance of the basic signature scheme built by Nikolay A.

2. Constructing the Related Basis Digital Signature Schemes

In this part, we use the problem of finding roots modulo in the finite ground field, with modulo p with the structure $p = Nt_0t_1t_2 + 1$, to build a collective digital signature scheme and a group digital signature scheme. These are the two basic signature schemes that we use to build the proposed collective digital signature schemes.

2.1 The Collective Signature Scheme Based on Problem of Finding Roots Modulo (The CDS-2 Scheme)

Assume there is a collective of members who sign the document M. The private keys and public keys of each signer in this signing collective are (K_{1_i}, K_{2_i}), $K_{1_i} < p, K_{2_i} < p$, and $Y_i = K_{1_i}^{w_1} K_{2_i}^{w_2}$, with $w_1 = t_0t_1$, $w_2 = t_0t_2$, $t_0 \approx t_1 \approx t_2 \approx 80$ bits and Note that the signer's private key is a tuple of two components.

The collective public key used in the verification of the collective signature is calculated by the formula $Y = \prod_{i=1}^{m} Y_i \bmod p$. is a pre-specified one-way secure hash function.

The process of checking the validity of a collective signature is the same as that of an individual signature [20].

The following are the procedures of the scheme [17].

The procedure for generating the collective digital signature on the document M

Includes the following stages:

1) Each i-th signer performs the following steps:

- Generate pairs of random numbers and (act as a pseudo-secret key)
- Calculate the value of according to the formula:
- Send to all other signers in the signing collective

2) A certain signer, or all, in the signing collective does:

- Calculate the value R according to the formula:

R acts as the general random component of the signing collective with the contribution of the random components R_i of each member of this collective.

- Calculate the value according to the formula:
- Send to all other signers in the signing collective

e is the first element of the collective signature.

3) Each i-th signer goes on to:

- Calculate their share signature component and according to the formulas:

$S_{1_i} = T_{1_i} K_{1_i}^{-e} \bmod p$

$S_{2_i} = T_{2_i} K_{2_i}^{-e} \bmod p$

- Send S_{1_i} and S_{2_i} to all other signers in the signing collective.

4) A certain signer, or all, in the signing collective does the final job: Calculate the second component and the third component of the collective signature according to the formulas

So the triple value is the collective signature of the signing collective consisting signerdocument M.

The procedure for verification the collective digital signature on the document M

To check the validity of the signature received with the document M, the verifier performs the following steps:

1) Calculate the value of the collective public key Y according to the formula:

2) Calculate the value of according to the formula:

$R^{'} = Y^{e} S_1^{w1} S_2^{w2} \bmod p$

3) Calculate the value of according to the formula:

$e' = F_H(M||R^{'}||Y)$

4) Compare with e. If The received signature is valid; otherwise, it is invalid and will be rejected.

Proof of the correctness of the CDS-2 scheme:

To prove the correctness of this scheme, we need to prove the existence of the test expression in the signature checking procedure.

Conspicuously, the test expression $e' = e$ always exists.

Indeed:

as so $e^{'} = F_H(M||R'||Y) = F_H(M||R||Y) = e$

Thus, the test expression $e^{'} = e$ always exists: This proves that the correctness of the signature check procedure, or the correctness of the CDS-2 scheme, is always guaranteed.

2.2 The Group Signature Scheme Based on Problem of Finding Roots Modulo (The GDS-2 scheme)

Assume there is a group of members who sign the document M. The private keys and the public key of each signer in this signing group are (K_{1_i}, K_{2_i}), $K_{1_i} < p, K_{2_i} < p$, and $Y_i = K_{1_i}^{w1} K_{2_i}^{w2}$, with $w_1 = t_0 t_1$, $w_2 = t_0 t_2$, $t_0 \approx t_1 \approx t_2 \approx 80$ bits and The private keys and the public key of the group manager (GM) are $K_1^{'}$, $K_2^{'}$, $K_1^{'} < p, K_2^{'} < p$, $w_1 = t_0 t_1$, and $Y^{'} = K_1^{'w1} K_2^{'w2}$.

The group public key used in the verification of the group signature is calculated by the formula

$Y = \prod_{i=1}^{m} Y_i \bmod p$. is a pre-specified one-way secure hash function.

The process of checking the validity of a group signature is the same as that of an individual signature [20]. The following are the procedures of the scheme:

The procedure for generating the group digital signature on the document *M*

Includes the following steps:

1) The GM does the following:

- Calculate the hash value of the document M using the formula
- Calculate mask coefficients λ_i for each signer in the group sign according to the formula:

$\lambda_i = F_H(H \,||\, Y_i || \, F_H(H \,||Y_i||K_1^{'}||K_2^{'}))$

- Send to each corresponding signer
- Calculate the first component of the group signature

2) Each i-th signer in the signing group does:

- Randomly generate pairs of numbers and and then calculate according to the formula:

$R_i = T_{1_i}^{w1} T_{2_i}^{w2} \bmod p$

- Send the value to the group manager

3) The GM continues to make:

- Generates a random value pair and and calculate the values $R^{'}$, and e according to

$e = F_H(M||R||U) \bmod \delta$

Where δ is a prime number of length $|\delta| = 160$ bits.

e is the second component of the group signature.

○ Send the value of to all signers in the signing group

4) Each signer continues to do the following:

- Calculate the shared signature component of S_{1_i}, ac-

cording to the formula

- Send the value to other signers in the signing group

5) The GM does the final work:

- Check the correctness of the shared signature of all signers in the signing group using the
- If all pairs of numbers are satisfied: Calculate the signature component of a personal share according to the following formulas:
- Calculate the third component $S_1$and the fourth S_2 of the group signature according to the following formulas:

So the set of values is the group signature of the signing group on the document M.

The procedure for verification the group digital signature on the document M

To check the validity of the signature received with the document M, the verifier performs the following steps:

1) Calculate the value of the group public key according to the formula:

2) Calculate the value of R^* according to the formula:

3) Compare the value of with e. If $e^* = e$: The received signature is valid; Otherwise, the received signature is invalid, it is rejected.

Proof of the correctness of the GDS-2 scheme:

To prove the correctness of this scheme, we only need to prove the existence of the check expression in the signature check procedure.

Conspicuously, the test expression always exists.

We have:

$R^* = \left(UY^{'}\right)^{e} {S_1}^{w1} {S_2}^{w2} \, mod \, p$

Because of so $e^* = F_H(M||R^*||U) = F_H(M||R||U) = e$.

So the expression always exists: This proves that the correctness of the signature check procedure, or the correctness of the GDS-2 scheme, is always guaranteed.

3. Constructing The Proposed Collective Digital Signature Schemes Based on Problem of Finding Roots Modulo in The Finite Ground Field

In this section, we use the collective digital signature scheme and the group signature scheme described in section 2 as the basis schemes to build two types of the proposed collective signature scheme: i) The collective digital signature scheme for many signing groups; and ii) The collective digital signature scheme for many signing groups and many individual signers.

3.1 Constructing the Collective Digital Signature Scheme for Signing Groups (The RCS.01-3 Scheme)

This section uses the two schemes just described above as the basis to build a representative collective signature scheme, the first type: The collective signature for many signing groups.

This scheme allows the creation of a collective signature on the document M which represents a signing collective with signing groups, each of which consists of members, which is controlled by the group manager (GM). The signature formation process is run by the group managers.

The input parameters, public keys, and private keys are selected, calculated as the base schemes above. The following are the procedures of the scheme [20].

The procedure for generating the collective digital signature for g signing groups on the document M

1) Each GM in the signing collective does the following:

- Calculate mask coefficients for the signers in the j-th signing group according to the formula:

  $\lambda_{ji} = F_H(H \, ||Y_i|| \, F_H(H|| \, Y_i|| \, K_1^{'}||K_2^{'}))$

(λ_{ji} is the mask coefficient of the i-th signer in the j-th signing group)

- Calculate the value of the component of the j-th signing group according to the formula:

U_j is considered as the shared value of the j-th signing group in the first component of the collective signature for the signing groups.

- Calculate the random component using the formula:
- Send and values to all other GMs in the signing collective

2) A certain GM in the singing collective, or all, computes the values of the and compoof the collective signature according to the following formulas:

and

$e = F_H(M||R||U) \, mod \, \delta$

Where δ is a large prime bits.

U and are the first and second components of the collective signature.

3) Each GM in the signing collective continues to do:

- Calculate the shared signature S_{1_j}, of the j-th signing group according to the formula:

with is the shared signature of the i-th individual in the j-th group.

- Send S_{1_j}, to other GMs in the signing collective

4) A certain GM in the signing collective, or all, does the following:

- Check the correctness of the shared signature of all signing groups in the signing collective
- If all are satisfied: Calculate the third and fourth components of the collective signature according to the formulas:

So set of values is the collective signature of signing groups on the document M.

The procedure for verification the collective digital signature for signing groups on the document M

To check the validity of the signature received with the document M, the verifier performs the following steps:

1) Calculate the collective public key of the signing collective according to the formula:

2) Calculate the value of the random component R^* according to the formula:

$R^* = (UY_{col})^e {S_1}^{w1} {S_2}^{w2} \ mod \ p$

3) Calculate the value of e^* according to the formula:

$e^* = F_H(M||R^*||\ U)$

4) Compare with e. If $e^* = e$: The received signature is valid; Otherwise, the received signature is invalid, it is rejected.

Proof of the correctness of the RCS.01-3 scheme:

The precision of this representative collective signature scheme is shown through: i) The existence of a shared signature verification formula shared by the signing team leaders R_j; and ii) Existence of the test expression in the signature check procedure. Specifically as follows:

a) Prove the correctness of the shared signature check formula:

It is easy to see that the formula for checking shared signature shared by team leaders signing always exists. Indeed:

Because of so $e^* = F_H(M||R^*||U) = F_H(M||R||U) = e$.

So the expression always exists: This proves that the correctness of the signature check procedure is always guaranteed.

From (a) and (b): The correctness of the RCS.01-3 scheme is guaranteed.

3.2 Constructing the Collective Digital Signature Scheme for Signing Groups and Individual Signers (The RCS.02-3 Scheme)

This section uses the two schemes just described above as a basis to build a representative collective signature scheme, the second type: The collective signatures for many signing groups and many individual signers.

This scheme allows the creation of a collective signature on document M that represents a signing collective with m individual signers and signing groups, each of which consists of members which is controlled by the group manager (GM). The signature formation process is run by the group managers and individual signers.

The input parameters, public keys, and private keys are selected, calculated as the base schemes above. The following are the procedures of the scheme:

The procedure for generating the collective digital signature for g signing groups and individual signers on the document M

Includes the following steps:

1a) Each GM in the signing collective does the following:

is the mask coefficient of the i-th signer in the j-th signing group)

- Calculate the value of the component of the j-th sign group according to the formula:

U_j is the shared member of the j-th signing group to form the first part of the collective signature

- Calculate the random parameter R_j of the j-th signed group according to the formula:

R_j is a shared member of the j-th signing group to generate a random parameter of the collective signature..

- Send and values to all other managers and individual signers in the signing collective.

1b) Each individual who signs the j-th performs the following tasks:

- Choose 2 random numbers and T_{2_j} and calculate the random value R_j according to the formula:

$R_j = {T_{1_j}}^{w1} {T_{2_j}}^{w2} \ mod \ p$

- Send the value to all signers GMs and other individual signers in the signing collective.

2) A GM or a certain individual signing in the collective calculates the values of and acco following formulas:

Where is a large prime ($|\delta| = 160 \ bits$); $U_j = 1$ when $j = g+1, g+2, ..., g+m$).

U and are the first and second components of the group signature.

3a) Each GM in the signing collective continues to do:

- Calculate the shared component S_{1_j}, S_{2_j} of group according to the formula:

with $S_{1_{ji}}, S_{2_{ji}}$ is the shared component of the i-th signer in the j-th group.

- Send S_{1_j}, S_{2_j} for GMs and other individual signers in the signing collective.

3b) Each individual signer in the signing collective continues to do:

(the j-th ; $j = g+1, g+2, ..., g+m$)

- Calculate the share component according to the for-

mula:

$S_{1_j} = T_{1_j} K_{1_j}^{-e} \bmod p$

Send to other GMs and individual signers in the signing collective.

4) A GM or an individual in the signing collective doing:

- Check the validity of each according to the formulas:

$R_j = (U_j Y_j^{'})^{e} {S_{1_j}}^{w1} {S_{2_j}}^{w2} \bmod p$

with $j = 1, 2, ..., g$

and

$R_j = S_{1_j}^{w1} S_{2_j}^{w2} Y_j^{-e} \bmod p$

with $j = g+1, g+2, ..., g+m$

- If all are satisfied: The third component of the group signature will be calculated according to formulas:

So the set of values is the representative collective signature of a collective consisting og signing groups and individual signers on the document M. This type of signature is also known a collective signature shared by multiple groups and signed by many individuals. It represents this collective signing.

The procedure for verification the collective digital signature for signing groups and m individual signers on the document M

To check the validity of the signature received with the document M, the verifier performs the following steps:

1) Calculate the collective public key of the signing collective according to the formula:

2) Calculate the value of the random parameter R^* according to the formula:

$R^* = (UY_{col})^{e} {S_1}^{w1} {S_2}^{w2} \bmod p$

3) Calculate e^* using to the formula:

$e^* = F_H(M \parallel R^* \parallel U)$ Compare with e. If The signature received is valid; Otherwise, the received signature is invalid, it is rejected..

Proof of the correctness of the RCS.02-3 scheme:

The precision of this representative collective signature scheme is shown through: i) The existence of a formula to check the shared signature S_j of each signing group R_j^*; ii) The existence of the signature test formula shared by each individual signer and iii) The existence of the test expression $e^* = e$. Specifically as follows:

a) The correctness of the formula to check the shared signature of each group leader:

It is easy to see that the formula for checking shared signature shared by team leaders signing always exists. Indeed:

$R_j = \left(U_j Y_j^{'}\right)^{e} {S_{1_j}}^{w1} {S_{2_j}}^{w2} \bmod p$

b) The correctness of the formula to check the shared signature per signer:

It is easy to see that the formula for checking the shared signature shared by the R signing team leaders always exists. Indeed:

e representative collective signature check procedure:

Conspicuously, the signature check expression always exists.

We see:

So the expression always exists. This proves that the correctness of the signature check procedure, or the correctness of the RCS.02-3 scheme, is always guaranteed.

4. Security Analysis and Performance Evaluation

4.1 Security Advantages of the Proposed Collective Signature Schemes

The group signature scheme we described in Section 2.2 has the following security advantages:

- As the scheme is based on the properties of the prime modulo root problem in a finite field, it inherits the safety level of this difficult problem. The attack resistance of the GDS-2 scheme is completely similar to the basic scheme described by Nikolay A. To circumvent this scheme, the attacker must find the prime modulo roots to simultaneously determine the two secret values and K_2.
- The public key of all signers, including the group manager, is "masked" by the mask parameter λ. The attacker will not be able to determine who in the signing group participated in the signing to form the group signature.
- The U component of the group signature contains information about all members of a signing group who took part in forming the group signature for this signing group. Consequently, when there is a dispute about the group signature, the group leader will be able to identify the signer easily later and resist the "disclaimer".
- There is no need to exchange or share security values, private keys, or secret keys between members of a signing group or between members of a signing group with the manager. Therefore, the Internet environment is sufficient to implement this scheme. In addition, the scheme is also easy to deploy on top of existing PKI (Public Key Infrastructure) systems [21].
- As shown in the 5th step of the signature generation procedure, a group manager only proceeds when he or she believes or has verified that all signatures participating in creating the collective signature are

valid. The operation generates the final component (S_1, S_2) of the group signature, by adding the shared signature of the group leader to the product of the shared signatures of all members. This makes it very hard to simulate member signings, or members signing each other's signatures and also shows the representativeness as well as high responsibility of the team manager.

The representative collective signature schemes built in this paper use the CDS-2 collective signature scheme and the GDS-2 group signature scheme as the basic scheme, so it also has the advantages of security and resistance to attacks like these schemes.

4.2 Performance of the Proposed Collective Signature Schemes

We evaluate the computational performance of the proposed representative collective signature schemes by calculating the time cost that the scheme takes for the signature generation process (Signature generation procedure) and the need for the signature verification process (Signature verification procedure). The time costs of representative collective signature schemes proposed in this paper are shown in Table 1.

Notations: Time cost of a hash operation in Z_p; Time cost of a scalar multiplication in Z_p; Time cost of a inverse operation in Z_p; Time cost of an exponent operation in Z_p; Time cost of a modular multiplication in Z_p.

$T_h \approx T_m, T_s \approx 29T_m, T_{inv} \approx 240T_m, T_e \approx 240T_m, T_{sqrt} \approx 290T_m$.

Information from Table 1 shows that the time cost for signature generation and signature checking of a proposed representative signature scheme is not much larger when compared to the new collective digital signature schemes.

5. Discussion

- The signature generation procedure in the proposed representative collective signature scheme shows that it has all the security advantages of the collective signature generation procedure and the group signature generation procedure. This is one of the advantages of the representative collective signature schemes proposed by us.
- The basic requirement for multi-signature schemes is to record the information of everyone who participated in creating the signature of the group or the collective. This information is needed for the identification of the signer and against the signer's "disclaimer of responsibility" in the future. The group signature schemes and the representative collective signature schemes built here have met this requirement, the signer information is contained in the first component of the signature, the U component. The algorithm to identify the signer from the information contained in the U has been described.
- The use of the U-component of the representative collective signature is necessary, but this increases

Table 1. Time cost of the proposed collective signature scheme: RCS.01-3 and RCS.02-3

The scheme	Time for the signature generation	Time for the signature verification
RCS.01-3	$U = \sum_{j=1}^{g} (243m_j + 1)\, T_m$ $e = [\sum_{j=1}^{g} (481m_j + 481) + 1]T_m$ $S_1 + S_2 = \sum_{j=1}^{g} (1209m_j + 484)\, T_m$ $Sum = [\sum_{j=1}^{g} (1934m_j + 966) + 1]T_m$	$(724+ g)T_m$
RCS.02-3	$U = \sum_{j=1}^{g} (243m_j + 1)\, T_m$ $e = [\sum_{j=1}^{g} (481m_j + 481) + 481m + 1]T_m$ $S_1 + S_2 = [\sum_{j=1}^{g} (1209m_j + 484) +$ $1206m]T_m$ $Sum = [\sum_{j=1}^{g} (1934m_j + 966) + 1687m + 1]T_m$	$(724+ g + m)T_m$

the signature size. This is considered a limitation of the proposed scheme. We have proposed and built a two-component representative collective signature scheme, but we can only implement the scheme based on discrete logarithm problems. We are working to build this improved scheme based on the problem of finding roots modulo large primes.

6. Conclusions

Thus, in this paper, we build a collective signature scheme and a group signature scheme using the single digital signature protocol described via a two-component private key (K_1, K_2). Based on their computational difficulty, all three schemes are formed in order to find the modulo root of a large prime, with a prime modulo $p = Nt_0t_1t_2 + 1$, in a finite ground field.

The two signature schemes described above can then be used as the basis for building two different types of collective signature schemes: i) The collective digital signature scheme for many signing groups; and ii) The collective digital signature scheme for many signing groups and many individual signers. These two schemes fully inherit the attack resistance of the single signature scheme and the difficulty of finding the modulo root in a finite prime field, so the security of the scheme is always guaranteed. For all schemes built in this study, if the chosen modulo is 1024 bits, their security level will be 80 bits.

In this paper, we analyze and evaluate the proposed schemes based on their security benefits and computational performance. In the future, the design of a collective signature scheme will be based on the computational difficulty of finding roots modulo on the elliptic curve.

Funding

We received funding for this research from Duy Tan University, Danang, Vietnam. https://duytan.edu.vn/.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Radack, S., 2009. Updated digital signature standard approved as Federal Information Processing Standard (FIPS) 186-3. National Institute of Standards and Technology. FIPS Publication 186-3.

[2] Pieprzyk, J., Hardjono, Th., Seberry, J., 2003. Fundamentals of computer security. Springer-Verlag. Berlin.

[3] Chaum, D., Heyst, E., 1991. Group signatures. Advances in Cryptology - EUROCRYPT 91. Springer-Verlag. pp. 257-265.

[4] Xie, R., Xu, C., He, C., et al., 2016. A new group signature scheme for dynamic membership. International Journal of Electronic Security and Digital Forensics. 8(4).

[5] Alamélou, Q., Blazy, O., Cauchie, S., et al., 2017. A code-based group signature scheme. Designs, Codes and Cryptography. 82(1-2).

[6] Moldovyan, A.A., Moldovyan, N.A., 2014. Group signature protocol based on masking public keys. Quasigroups And Related Systems. pp. 133-140.

[7] Moldovyan, N.A., Minh, N.H., Hung, D.T., et al., 2016. Group signature protocol based on collective signature protocol and masking public keys mechanism. International Journal of Emerging Technology and Advanced Engineering. 6, 1-5.

[8] Tuan, N.K., Van, V.L., Moldovyan, D.N., et al., 2018. Collective signature protocols for signing groups. Proc. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, India.

[9] Tuan, N.K., Duy, H.N., Moldovyan, N.A., 2021. Collective Signature Protocols for Signing Groups based on Problem of Finding Roots Modulo Large Prime Number. 13(4), 59-69.

[10] Camenisch, J.L., Piveteau, J.M., Stadler, M.A., 1995. Blind signatures based on the discrete logarithm problem. Proc. Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, Berlin Heidelberg New York. pp. 428–432.

[11] Chaum, D., 1983. Blind signatures for untraceable payments. Proc. Advances in Cryptology – CRYPTO'82, Plenum Press. pp. 199–203.

[12] Moldovyan, N.A., Moldovyan, A.A., 2010. Blind collective signature protocol based on discrete logarithm problem. International Journal of Network Security. 11(2), 106-113.

[13] Tuan, N.K., Duy, H.N., Moldovyan, N.A., 2021. Constructing the 2-Element AGDS Protocol based on the Discrete Logarithm Problem," International Journal of Network Security & Its Applications. 13(4), 13-22.

[14] Itakura, K., Nakamura, K., 1983. A public key cryptosystem suitable for digital multisignatures. NEC Research and Development. 71, 1-8.

[15] Tuan, D.M., 2012. New elliptic curve digital multi-signature schemes for multi-section messages. Proc. International Conference on Computing and Communications Technologies Research - Innovation

and Vision for the future, Viet Nam. pp. 25-28.

[16] Poulakis, D., Rolland, R., 2015. A digital signature scheme based on two hard problems. Computation, Cryptography, and Network Security, Springer. pp. 441-450.

[17] Moldovyan, N.A., 2008. Digital Signature Scheme Based on a New Hard Problem. Computer Science Journal of Moldova. 16(2), 163-182.

[18] Bolotov, A.A., Gashkov, S.B., Frolov, A.B., 2006. Elementary introduction to elliptic curve cryptography. Cryptography Protocols on The Elliptic Curves. KomKniga, Moskow.

[19] Johnson, D., Menezes, A.J., Vanstone, S., 2001. The elliptic curve digital signature algorithm (ECDSA). Certicom.

[20] Moldovyan, N.A., Shcherbacov, V.A., 2012. New signature scheme based on difficulty of finding roots. Quasigroups and Related Systems. 20, 261-266.

[21] Yong, H., Fugui, C., Peixin, Q., 2009. Research on Digital Signature Based on Digital Certificate. Proceedings of 14th Youth Conference on Communication, Scientific Research. pp. 467-470.

[22] Popescu, C., 1999. Blind signature and BMS using elliptic curves. Studia Univ Babes–Bolyai. Informatica. pp. 43-49.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems
https://ojs.bilpublishing.com/index.php/jeis

ARTICLE

Ge-based Medium Wave Infrared MCT 1280 × 1024 Focal Plane Detector

Jun Jiang*

Kunming institute of physics, Kunming, Yunnan, 650223, China

ARTICLE INFO

Article history
Received: 17 December 2021
Accepted: 10 March 2022
Published Online: 25 March 2022

Keywords:
Germanium substrate
Megapixel
Mercury cadmium tellurium
Medium wave focal plane detector
Back thinning

ABSTRACT

Medium-wave HgCdTe thin films grown on germanium-based substrates by molecular beam epitaxy were treated by large area n-on-p injection junction and flip-flop mixing process. The chips interconnected with low-noise and multimodal options readout circuit composed a 1280×1024 Medium-wave Infrared Focal Plane Cooling Detector whose pixel spacing was 15 microns. Its main photoelectric properties are average NETD equivalent to 18.5 mK, non-uniformity equivalent to 7.5%, operability equivalent to 98.97%. The paper also studies the substrate-removal technique on Germanium-based chip, which improves the stability and reliability of detector.

1. Introduction

Infrared technology is a photoelectric conversion technology that converts infrared radiation into identifiable electrical signals. It is one of the key technologies to realize the informatization of high-tech equipment. Infrared detector is the core of infrared technology. Its quality and characteristics determine the performance and level of equipment. Infrared detector has the advantages of long operating distance, good anti-interference, strong ability to penetrate smoke and haze, and can work all day. It has been widely used in military and civil fields.

In recent years, in order to achieve high spatial resolution, large-scale and super large-scale infrared focal plane detector components have attracted great attention. As a megapixel focal plane detector with the typical characteristics of the third generation focal plane, it is widely used in aviation, aerospace and other aspects [1].

Traditional infrared focal plane detectors mostly use CdZnTe Single crystal wafer with good lattice matching with HgCdTe photosensitive material as epitaxial substrate. However, due to the characteristics of long process cycle, low crystallization rate, small ingot size and low yield of CdZnTe Single Crystal [2], the price of epitaxial

*Corresponding Author:
Jun Jiang,
Kunming institute of physics, Kunming, Yunnan, 650223, China;
Email: jj.wjy@163.com

DOI: https://doi.org/10.30564/jeisr.v4i1.4232

CdZnTe substrate is high. In order to overcome the problems of small size and high chip preparation cost of traditional HgCdTe epitaxial materials, ultra large scale focal plane arrays are prepared by germanium based HgCdTe materials, which have obvious advantages in the preparation of megapixel focal plane detectors.

2. Design and Process Realization of Germanium Based Medium Wave HgCdTe Focal Plane Detector Assembly

2.1 Medium Wave HgCdTe Thin Film Material Molecular Beam Epitaxy on Germanium Based

The epitaxial HgCdTe material on Ge substrate faces many technical challenges, among which the biggest problem is that the lattice mismatch is as high as 14%, which makes the problems such as epitaxial layer crystal direction control, high-density dislocation suppression and surface defect density suppression particularly prominent [3]. Around these problems, the high-precision calibration and control of growth temperature, substrate material pretreatment technology structure design and growth of composite buffer layer, large area HgCdTe material epitaxy process, HgCdTe material heat treatment technology and other core processes.

The surface state of Ge substrate directly affects the quality of epitaxial layer and the number and size of surface macro defects [4]. The carbon particles on the surface need to be removed at a high temperature of 1200 ºC, which is difficult for MBE equipment, and carbon may form surface macro defects, so how to remove carbon becomes the key of Ge substrate epitaxy. The epitaxial HgCdTe material on Ge substrate also faces many technical challenges. The biggest problem is the serious lattice mismatch, which makes it very difficult to control the crystal orientation of epitaxial layer, suppress high-density dislocations and suppress the density of surface macro defects. Around these problems, through low-temperature oxide layer removal technology, epitaxial layer polarity control technology, atomic layer epitaxy technology The atomic level flat surface is obtained by epitaxy technology at extreme temperature, high temperature annealing technology, crystal deflection angle and increasing surface atomic step density.

At the same time, through a large number of experiments, an effective Ge substrate cleaning and corrosion process was found out. Combined with vacuum low-temperature deoxidation and as monolayer Ge surface passivation process, an atomic level flat surface suitable for epitaxial growth was obtained.

Due to the different crystal properties of germanium and HgCdTe materials, there is a large defect density. It is necessary to control the interface layer of germanium and HgCdTe through appropriate design and process, control the lattice mismatch and other defects in the interface buffer layer, and suppress the material defects in the HgCdTe photosensitive layer. In the study, HgTe/CdTe alternating structure (20 cycles) was used to improve the EPD of MCT materials. On the composite substrate after the growth of CdTe buffer layer, before the growth of MCT materials, the HgTe/CdTe alternating layer with a long period of 20 cycles was used, as shown in Figure 1.

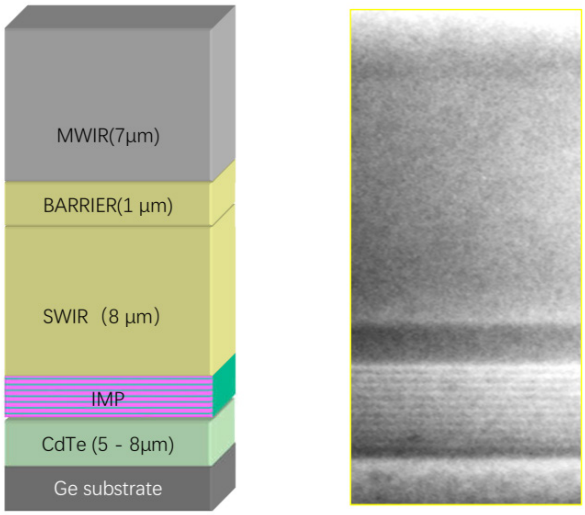


Figure 1. HgTe/CdTe composite buffer layer structure

For the growth of CdTe on large mismatch Ge substrate, there are four main problems: one is that large mismatch causes high dislocation density; The second is that twins are very easy to appear. The research shows that for heteroepitaxy with large lattice mismatch, large mismatch leads to higher surface energy at the interface, The system will deflect and grow in the direction of reducing the energy of the system (i.e. growing towards the crystal surface with low surface energy). The greater the degree of fit, the easier it is to produce polycrystals or twins, resulting in three-dimensional growth mode, which seriously affects the crystal quality. Therefore, the main reason for the formation of twins is the high interface energy caused by large lattice mismatch; the third is the large thermal mismatch between the substrate and CdTe epitaxial layer, which will lead to the generation of stress in the epitaxial layer. The fourth is non-polar To grow polar CdTe on Ge substrate, a non-polar surface needs to be prepared on the surface of clean Ge substrate after high temperature deoxidation.

Large area uniform HgCdTe growth, using Ge single crystal as epitaxial substrate, The lattice mismatch be-

tween Ge single crystal and HgCdTe is large (the mismatch is about 14.6%), so we must epitaxial a layer of CdTe with a certain thickness on Ge as a buffer layer, and then epitaxial HgCdTe. The dislocations on the CdTe surface will extend into the HgCdTe layer grown on it, which will directly affect the HgCdTe crystal quality. In order to determine the relationship between the dislocation density on the CdTe surface and the thickness of the epitaxial layer, we conducted X-ray bicrystal analysis of CdTe epitaxial layers with different thicknesses Swing back curve FWHM measurement and EPD study. It is found that when the thickness is greater than 6μm, FWHM changed slowly, and the surface EPD value decreased to (7 ~ 9) × 106cm^{-2}, which no longer decreases significantly with the further increase of thickness.

The composite buffer layer with HgTe/CdTe alternating structure is selected. Most of the screw dislocations caused by substrate mismatch are pinned in the alternating structure of 20 cycles. Therefore, the EPD of the subsequently grown multilayer MCT material is significantly controlled, which can reach 2.5×10^6 / cm^2 level.

Stable MBE growth temperature is the key factor for the epitaxy of high-quality multilayer HgCdTe films. The growth temperature affects the adhesion coefficient of Hg on the substrate surface and directly determines whether the growth condition is Hg deficient or Hg rich. The number and size of macro defects on the material surface are closely related to the state of Hg. The appropriate growth temperature also determines the crystal quality and corrosion pit density of MCT films.

Through the theoretical simulation of different growth surfaces, the optimal temperature change curve of growth is obtained. Based on this, the heating power is compensated during the growth process, so that the temperature is stable at ± 3 ºC during CdTe growth and ± 1 ºC during MCT growth.

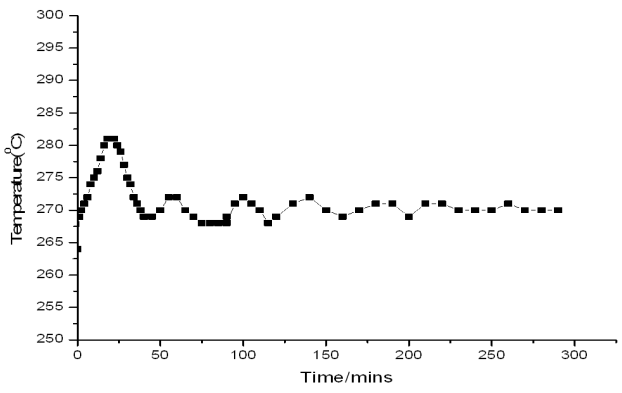


Figure 2. Temperature change curve measured by power compensated CdTe mid infrared thermometer

Through the above research, the properties of Ge based MBE HgCdTe thin films are as follows: half peak width: 90 ~ 110arcsec; Corrosion pit density: ~ 2.5 × 10^6/cm^2; Surface macro defect density: ~ 300 / cm^2 (< 10 μm).

2.2 Process Realization of Detector Chip

Ge base 1280×1024 HgCdTe photovoltaic detector chip is the core and key of detector module. In the preparation of detector chip, a single-layer p-type large-area HgCdTe material doped with Hg vacancy is used to form the detector photosensitive element array by ion implantation. The plane junction technology is adopted, and the pixel center distance is 15 μm. The structure is shown in Figure 3.

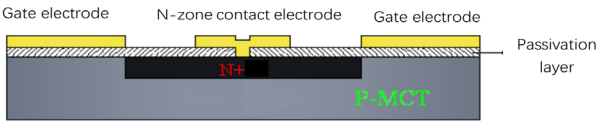


Figure 3. Photosensitive element structure

The research of detector chip is based on mature technologies such as material surface treatment, passivation, ion implantation, high-precision lithography, flip chip interconnection, dry etching and back thinning. It focuses on core processes such as high-performance surface passivation, large-scale high-density and high-reliability interconnection technology.

Good surface passivation process can effectively reduce the surface damage of HgCdTe, reduce the interface state of HgCdTe device surface, reduce the leakage current on the device surface, reduce the surface recombination speed and 1/f noise of HgCdTe device, improve the dynamic resistance and directional breakdown voltage of detector, and improve the performance of device [5]. Therefore, in the device process, the preparation of dense and high resistance passivation layer is studied. In this paper, the CdTe/ZnS composite passivation film system is adopted. In view of the imbalance between Cd and Te in the ordinary CdTe growth mode, the Te rich CdTe passivation film is obtained by adding high-purity Te technology, which effectively reduces the Hg rich defect state density on the surface of HgCdTe caused by heat treatment process and greatly reduces the dark current of the device, The dynamic resistance of the device is effectively improved. In the passivation process, a CdTe/ZnS composite passivation film with excellent surface roughness and adhesion was prepared by adjusting the RF power, target substrate distance and sample swing angle. The non-uniformity of the passivation film reached ± 4.3% in 3-inch samples. It provides a composite passivation film preparation process with better repeatability and consistency for

the preparation of large array HgCdTe devices.

In this paper, flip interconnect optical sensitive array chip and readout circuit (ROIC) are used for electrical connection, as shown in Figure 4. Due to the large scale of the developed array (1280×1024), more than 1.3 million interconnection points need to be welded. In the interconnection technology, not only the electrical and mechanical connection of the interconnection point should be ensured, but also the stress caused by the mismatch of thermal expansion between the detector chip and the silicon readout circuit under the cold and heat cycle should be buffered.

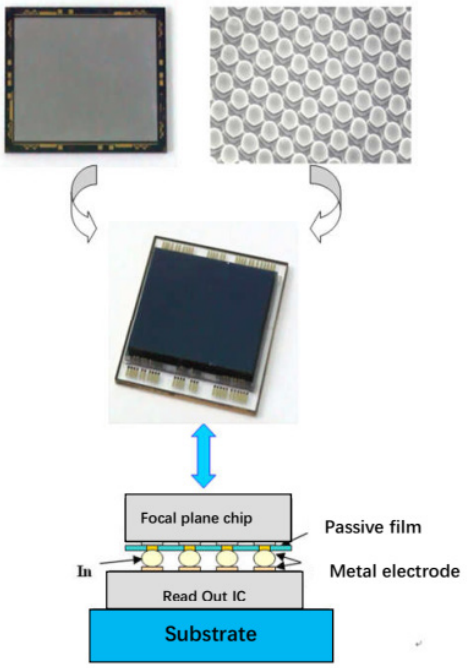


Figure 4. Schematic diagram of flip chip interconnection of focal plane detector

This paper focuses on solving the interconnection reliability between detector chip and readout circuit, improving the growth and molding process of indium column, strictly controlling the parallelism between silicon readout circuit and HgCdTe chip, and ensuring the high consistency of indium column; Secondly, the best process parameters for flip chip welding of various thickness chips, indium column height and large-scale chips are found out. After flip chip welding, epoxy glue is injected between the readout circuit and the chip to enhance the welding strength and effectively fill the gap between them. At present, the flip chip welding connectivity of indium column reaches 100%.

2.3 Readout Circuit Design

The readout circuit integrates, stores, cell gating, line gating, sample hold and high-speed output the instantaneous signal from the photovoltaic diode. The readout circuit adopts mature 0.35 μm CMOS technology, not only has the ability to realize various functions such as low-noise signal processing and output, but also has good low-temperature operating characteristics. The readout circuit has a variety of working modes, windowing and readout modes to meet different application requirements.

The readout circuit integrates, stores, unit gating, row gating and sample hold the signal (direct injection) from the photovoltaic diode, and adopts two working modes: integration before readout (ITR) and integration while readout (IWR), with optional output channels.

The readout circuit is designed with the window selection function. The circuit can select the window as full window or partial window according to the input signals sizea and sizeb (see Table 1).

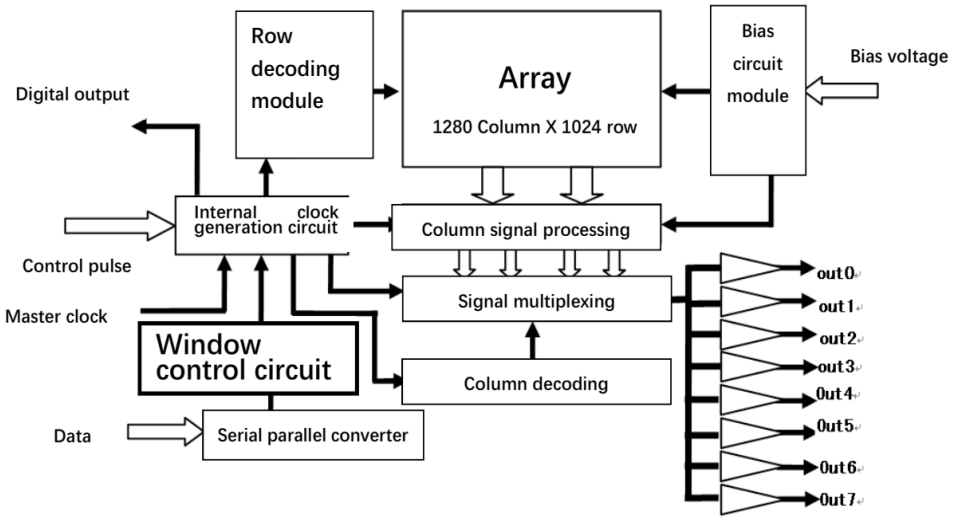


Figure 5. Functional module diagram of readout circuit

Table 1. Selection of working mode

SIZEA	SIZEB	Format
1	1	1280×1024 (default)
1	0	1280×960
0	1	1024×1024
0	0	1280×1024 window mode

In terms of reducing circuit power consumption, including reasonably setting the size of transistors in the operational amplifier circuit and driving the operational amplifier, through circuit design,the output of the medium wave readout circuit is 4 or 8 channels. When the output is 4 channels, the Output Op Amp of the remaining 4 channels stops working, rather than simply shielding the input/output of the four channel op amp signals with a switch, so as to greatly reduce the power consumption of the circuit.

Due to the increase of readout circuit array, how to improve the consistency of pixel circuit in a limited area has become a difficulty in circuit design. The expansion of readout circuit array will prolong the circuit signal output time, make the capacitor hold signal time longer, and cause the signal uniformity to deteriorate. Therefore, the integral and hold capacitance are appropriately increased in the design. However, due to the limited chip area, the chip area, capacitor charge and discharge time and other factors are comprehensively considered in the design, and the capacitance value is reasonably set, To improve the uniformity of pixel circuit.

2.4 Germanium Based Back Thinning

The focal plane detector in this paper needs to work near the temperature of 80 K. When the refrigerator cools the detector chip from the ambient temperature to the working temperature of the detector chip in a short time, the temperature difference during the cooling process changes by more than 200 K. Due to the mismatch of parameters such as material expansion coefficient, elastic modulus and Poisson's ratio, the detector chip, readout circuit and Dewar loading substrate, Cause the chip to bear great stress and deformation [6]. In this paper, the structural deformation of dewar cold head detector chip and loading substrate under cooling state is simulated and analyzed, as shown in Figure 6. When the detector chip is cooled to 80 K in a short time, the structural deformation caused by drastic temperature change reaches 10 μm or so. This deformation is mainly caused by the thermal mismatch between the chip and the readout circuit, which is often easy to cause serious consequences such as the rapid increase of bad pixels of the detector chip or chip cracking. Therefore, the back thinning process is a necessary process link for a highly reliable hybrid staring focal plane detector, which can minimize the thermal mismatch between the chip and the readout circuit, improve the reliability of the module, and meet the environmental adaptability requirements of complex and harsh environment applications. Therefore, we must improve the flexibility of the chip itself by thinning the back of the chip, so as to improve the ability of the chip to withstand stress and

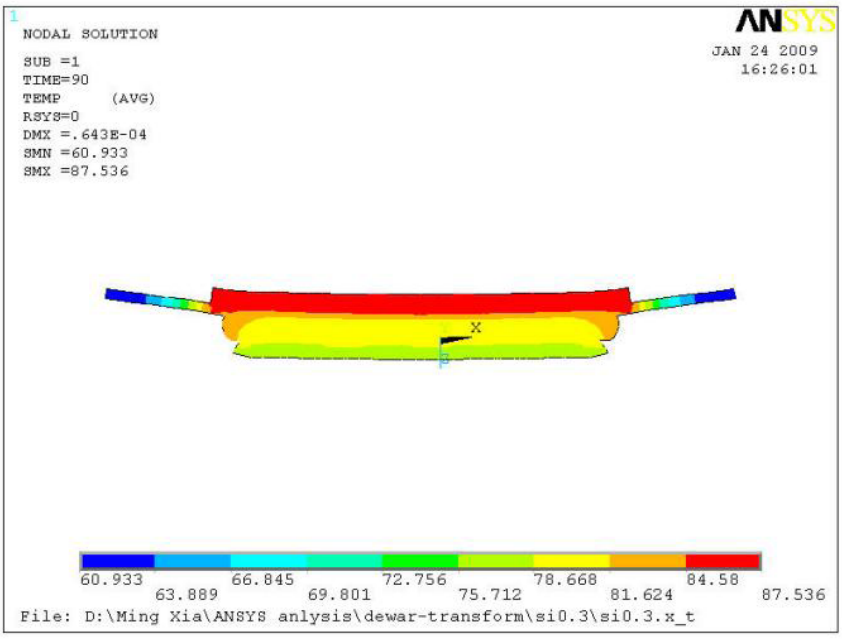


Figure 6. Finite element analysis of chip deformation under cooling state

deformation, and improve the ability of the chip to resist the temperature impact of the refrigerator on and off.

In the process research of Ge based back thinning, a highly reliable filling process is carried out between the light sensitive array chip and the readout circuit. The focal plane chip is filled with filling polymer with good fluidity and stable at low temperature, so as to strengthen the support strength of the chip and further reduce the thermal mismatch of the chip. By means of mechanical turning, the germanium substrate is thinned with low damage and low stress, the whole germanium substrate is completely removed, and the mismatch between germanium substrate and silicon readout circuit caused by inconsistent thermal expansion is reduced. At the same time, the germanium substrate thinned to a certain thickness is finally treated by wet chemical process to remove the damage caused by mechanical thinning, and provide a good interface for the sputtering of back antireflection film.

Through the above mechanical and chemical back subtraction process research, the low damage back subtraction removal of large area array Ge based substrate has been realized. It can be seen from Table 2 that the performance of the device does not decline significantly before and after back substrate removal.

Table 2. Ge base 1280 × Performance comparison of 1024 focal plane detector before and after back substrate removal

	before	after
Bad pixel rate	1.74%	1.85%
NETD	22.3 mK	24.5 mK
non-uniformity	8.1%	7.9%

2.5 Dewar Design

The Dewar of the detector assembly is to Ge based medium wave 1280×1024 focal plane detector chip provides an all metal vacuum packaging structure, which can make the detector chip work in a 77 K vacuum environment after matching with the refrigerator. At the same time, Dewar also provides an optical transmission channel for transmitting infrared radiation, which includes the optical window of Ge material, filter and aperture. The filter is coated with a band-pass optical film to limit the transmission of a specific infrared wavelength, and the aperture is used to limit the optical aperture (F#) of the detector, which is usually matched with the imaging lens.

In the design of Dewar, the principles of universality, small volume, light weight and high reliability are fully considered. The all metal integrated structure is adopted. The high-strength and low thermal conductivity thin-walled metal inner tube is integrated with the refrigerator. The high air tight HTCC ceramic lead ring is directly interconnected with the loading substrate. The electroforming process realizes the manufacture of high-strength ultra-thin aperture. The aperture adopts high-strength ultra-thin multi-layer structure. The aperture not only ensures the optical F# but also increases the multi-layer impurity elimination to aperture improve the cold shielding efficiency. All parts of Dewar adopt strictly controlled surface treatment process to ensure vacuum service life and reliability.

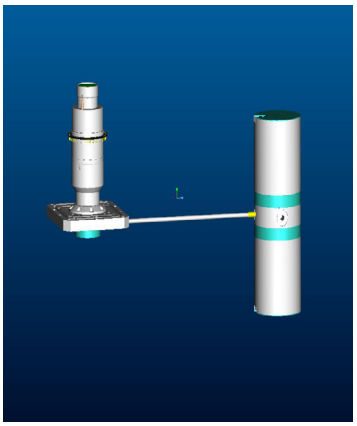


Figure 7. Design structure of Dewar

In order to effectively reduce the background radiation noise, the v adopts a multi-layer anti stray light structure, and the multi-layer structure is also conducive to the improvement of the structural strength of the aperture. Improving the emissivity of the blackened layer on the inner surface of the aperture can improve the ability to absorb secondary and multiple reflected stray light. The emissivity of the blackened coating is higher than 95%, which can minimize the infrared background radiation and improve the detection rate, so as to improve the quality of thermal imaging.

ANSYS and other simulation software are used to analyze the stress and deformation of the cold head structure, optimize the structure, metal coating and contact surface shape of each Dewar part in the cold head laminated structure, determine the selected materials of each part, and ensure the temperature uniformity of the loading surface of the detector. By continuously optimizing and improving the materials and structures of metal negatives, transition blocks and loading substrates, the optimal combination of cold head structure is achieved. The temperature distribution diagram of the cold head before and after the optimization and improvement of the dewar cold head structure. The temperature difference on the loading surface is reduced from 2.26 K to 0.8 K (see Figure 8), which significantly improves the temperature uniformity of the

loading surface and significantly reduces the deformation and stress of the detector chip.

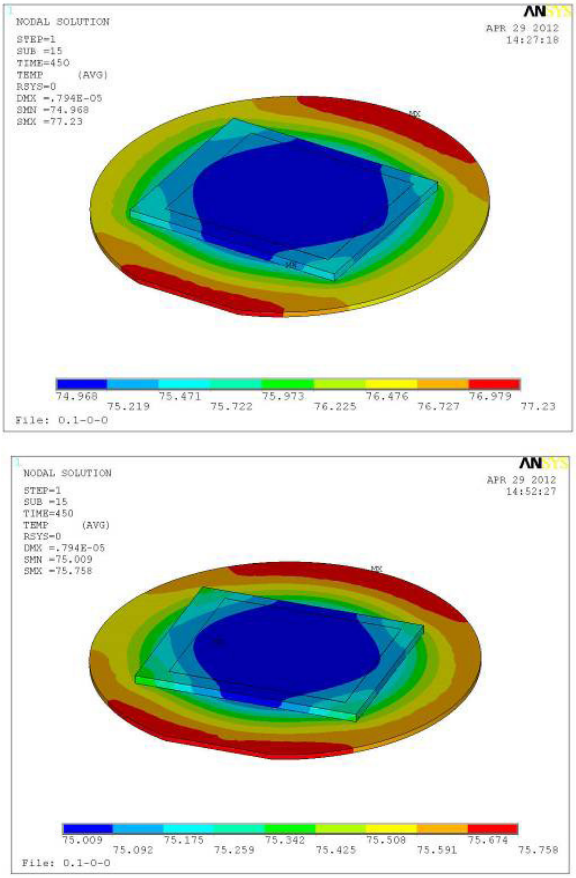


Figure 8. Cold head temperature distribution before and after Dewar design improvement

3. Component Performance and Environmental Test

Developed Ge based medium wave 1280×1024 focal plane detector is packaged in metal dewar and connected with Stirling refrigerator. The photoelectric performance of the module is tested. The main technical indexes are: working temperature 81 K, average NETD 18.5 mK, non-uniformity 7.5% and bad pixel rate 1.27%.

The environmental adaptability of the module is studied. The environmental test includes high-temperature storage, low-temperature storage, high-temperature impact, low-temperature impact, high-temperature work, low-temperature work, mechanical impact and impact. Specific environmental tests are as follows:

High temperature storage: storage temperature +71 ºC for 24 h.

Low temperature storage: storage temperature –54 ºC for 24 h.

High temperature operation: temperature +71 ºC, heat preservation for 1 h, operation for 2 h, and the temperature change rate shall not exceed 10 ºC/min.

Low temperature operation: temperature –40 ºC, heat preservation for 1h, operation for 2 h, and the temperature change rate shall not exceed 10 ºC/min.

Temperature shock: low temperature –54 ºC± 2 ºC, high temperature + 71 ºC± 2 ºC, limit temperature maintained for 2 h, cycle for 3 times, and conversion time no more than 5 min.

Vibration: The component fulfills the specification during and after exposure to vibration in three mutually perpendicular axes during one hour per axis, with the following random profile to 5.33 g RMS. Between 5 Hz and 28 Hz, linear from 0.0026 g^2/Hz to 0.08 g^2/Hz. Between 28 Hz and 250 Hz, constant 0.08 g^2/Hz. Between 250 Hz and 2000 Hz, linear from 0.08 g^2/Hz to 0.00016 g^2/Hz. See Figure 9.

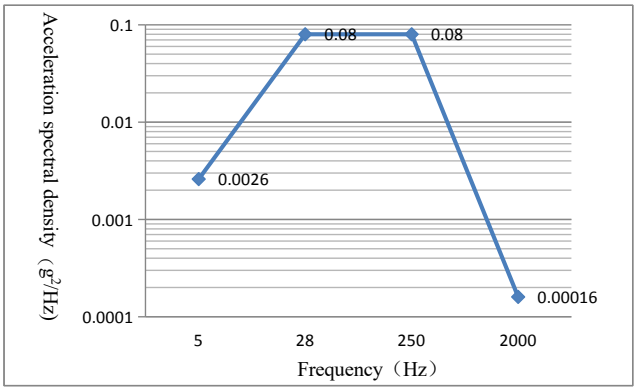


Figure 9. Random Vibration spectra

Mechanical shocks: The component fulfills the specification after exposure to shocks in each of the three mutually perpendicular axes with the following levels: 1/2sine 100 g 1 ms, with 3 shocks per axis per direction.; 1/2sine 50 g 6 ms, with 3 shocks per axis per direction; 1/2sine 40 g 18 ms, with 3 shocks per axis per direction; 1/2sine 25 g 6 ms, with 500 shocks per axis per direction.

The environmental test includes high-temperature storage, low-temperature storage, high-temperature impact, low-temperature impact, high-temperature work, low-temperature work, mechanical impact and shock. After the environmental test, the component performance has not changed significantly. At the same time, the performance of the components stored in the conventional environment for one year was retested, and there was no decline in performance.

4. Results & Discussion

In this paper, Ge substrate is used as the substrate of HgCdTe molecular beam epitaxy material, which replaces

CdZnTe substrate as the epitaxial substrate of HgCdTe material. Due to the high requirements of HgCdTe epitaxial film on the substrate, although CdZnTe and HgCdTe have small lattice mismatch coefficient, due to the low single crystal crystallization rate of CdZnTe and small ingot diameter. In particular, it is difficult to meet the requirements of large material substrate for large array HgCdTe infrared focal plane devices. At the same time, the growth cycle of CdZnTe crystal is long, about 40 days. Therefore, in the focal plane detector chip based on the traditional CdZnTe substrate, the qualified CdZnTe substrate accounts for the main cost of the detector chip. The production of HgCdTe thin film material by molecular beam epitaxy on Ge substrate has the advantages of low growth cost and short growth cycle. Therefore, using Ge based substrate instead of CdZnTe Single Crystal is expected to reduce the comprehensive cost of large area array infrared focal plane chip by more than 50%.

The above research results and related process methods can be applied to different specifications of Ge based medium wave array focal plane detector components. At the same time, it can also consider using Si substrate of the same material as readout circuit as the alternative substrate of CdZnTe to realize the preparation of low-cost infrared detector.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Nelms, N., Minoglou, K., Voland, C., et al., 2015. Visible and infrared detector development supported by the European Space Agency. Proceedings of SPIE. 9639, 96390O.

[2] Yang, J.R., 2012. Physics and technology of HgCdTe materials. Beijing: National Defense Industry Press.

[3] Li, Y.H., Yang, Ch.Zh., et al., August 2015. Molecular beam epitaxy CdTe films on 4-inch Ge substrates The 11th National molecular beam epitaxy conference.

[4] Yang, Ch.Zh., Li, Y.H., et al., August 2015. Pretreatment of 3-inch Ge (211) substrate for MBE growth. 2015 academic conference of China Optical Society.

[5] He, L., Yang, D.J., Ni, G.Q., et al., 2011. Introduction to advanced focal plane technology. Beijing: National Defense Industry Press.

[6] Tian, L.P., Zhu, Y.F., Liu, X.Y., et al., 2013. Infrared technology. 35(10), 629-631.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems
https://ojs.bilpublishing.com/index.php/jeis

ARTICLE

Numerical Simulation of Thermal Management of Lithium Battery Based on Air Cooled Heat Dissipation

Zhenhua Li*

Sangdun New Energy Technology Co., Ltd., Xiangtan, Hunan, 411202, China

ARTICLE INFO

Article history
Received: 27 December 2021
Accepted: 14 March 2022
Published Online: 25 March 2022

Keywords:
Lithium ion battery pack
Air cooled heat dissipation
Temperature field
CFD

ABSTRACT

In recent years, due to the rapid increase in the number of vehicles in the world, the traditional vehicles using gasoline or diesel as energy have led to serious air pollution and energy depletion. It is urgent to develop practical clean energy vehicles. The performance of electric vehicle depends on the power battery pack. The working temperature of the battery pack has a great impact on the performance of the battery, so it is necessary to carry out thermal management on the battery pack. Taking a lithium-ion battery as the research object, the temperature field of the battery pack in the charge and discharge state is simulated and analyzed by using CFD simulation software in the way of air cooled heat dissipation, so as to understand the influencing factors of uneven temperature field. At the same time, the development trend of battery temperature can be well predicted through simulation, so as to provide theoretical basis for the design of battery pack.

1. Introduction

Automobile is an important part of modern civilization. It not only promotes social development, but also causes increasingly serious energy crisis and environmental pollution. Severe energy and environmental challenges make the transformation of transportation energy become the main task faced by the automotive industry, and the electrification of automotive power system becomes an inevitable trend [1]. Battery pack is the only power source of pure electric vehicle. Its working performance is very important for electric vehicle, and the temperature of battery pack is also very important for the performance and service life of battery pack. The thermal management of battery pack directly affects the performance of the whole vehicle. If the temperature of the battery pack is too high and beyond the normal working range, the generation of irreversible substances in the battery pack will be accelerated. At the same time, due to the difference of working state of each battery unit, the temperature difference of the battery pack will be large, which will aggravate the difference of charge and discharge state of the battery pack, resulting in less cycle service life of the battery pack. When the temperature reaches the ignition point of the battery material, it will even cause the battery pack to catch fire; when the battery pack works at low temperature, dis-

*Corresponding Author:
Zhenhua Li,
Sangdun New Energy Technology Co., Ltd., Xiangtan, Hunan, 411202, China;
Email: 1957876517@qq.com

DOI: https://doi.org/10.30564/jeisr.v4i1.4279

charge efficiency of the battery pack will be reduced. The batteries of electric vehicles are connected in series. If the temperature of any single unit is too high or too low, it will affect the whole battery pack. If the battery pack is in the state of large temperature difference for a long time, the imbalance of battery capacity in the battery pack will affect the capacity of the whole battery pack. Therefore, thermal management must be carried out for the battery pack.

Simply changing the ventilation mode cannot achieve the best heat dissipation effect. In recent years, researchers all over the world have optimized the structure of the battery pack to improve the heat dissipation effect. In terms of air cooled heat dissipation, Anthony Jarrett et al. studied the heat dissipation plate structure of electric vehicle high-energy battery, and studied the use of air cooling to cool the battery pack, and optimized length and width of the cooling channel. CFD software is used for simulation to obtain the pressure drop and average temperature rise of cooling air, and then arbitrarily change the shape of cooling channel to compare the heat dissipation effect. The results show that any of the above designs can meet the requirements of fluid pressure drop and average temperature rise. By comparing the optimization results, they designed the cooling channel of the heat dissipation plate as a serpentine channel [2].

Kelly et al. conducted real vehicle test of power battery pack air cooling system based on Honda Insight and Toyota Prius. The experiment selected the working mode of the fan in real time according to the ambient temperature distribution of the battery in the battery pack. The experimental results show that the temperature difference between the battery cells of the two battery packs is small, and the ambient temperature of the battery pack is within the normal working temperature range of the battery pack. Khodadadi J.M. et al. studied the spacing between cells of the battery pack and the air inlet flow rate of the battery pack to optimize the maximum temperature and temperature uniformity of the battery pack, and compared the advantages and disadvantages in terms of heat dissipation effect and battery pack tightness through unilateral heat dissipation and bilateral heat dissipation experiments of the battery pack. Finally, a better heat dissipation model was obtained through mathematical analysis. Xu X.M. and He R. analyzed the influence of the inlet and outlet position of the battery pack and the battery layout on the battery heat dissipation effect, and studied the ventilation form of the battery pack through the battery pack heat dissipation experiment and software simulation analysis [3].

In this paper, the temperature rise characteristics of lithium-ion battery in charge and discharge state and the heat dissipation temperature field of battery pack in charge and discharge state are analyzed by combining theoretical analysis and simulation analysis, so as to ensure that the ambient temperature of battery pack is maintained in a certain range and improve the performance and safety of battery pack.

2. Temperature Field Simulation of Lithium Battery Pack

2.1 Establishment of Geometric Model of Battery Cell

The charging mode of power lithium battery generally adopts the mode of constant voltage and current limiting to avoid the battery exceeding the upper voltage limit. Under the condition of good control, the power lithium battery will not have side reactions during charging and discharging. Therefore, the internal reaction heat of power lithium battery have three parts: polarization heat Q_1, Joule heat and reaction heat Q_3. When the temperature of power lithium battery reaches 70 °C~ 80 °C, most of the total heat produced by the battery is reaction heat. When charging and discharging below the above temperature, most of the heat is Joule heat. Generally, the normal working temperature range of power lithium battery is –20 °C~ 65 °C. Therefore, the heat generation of power lithium battery during operation are mainly polarization heat and Joule heat Q_2 [4].

$$Q_a = Q_1 + Q_2 = I^2R_1 + I^2R_2 = I^2R_a \quad (1)$$

Where Q_a is the total calorific value of power lithium battery, J; I is the current during charging and discharging of power lithium battery, A; R_1 is the polarization internal resistance of power lithium battery, Ω; R_2 is the internal resistance when electrons flow in power lithium battery, Ω; R_a is the total internal resistance of power lithium battery during charging and discharging, Ω.

Heating power per unit volume of power lithium battery, that is body heat source:

$$q = Q_a/V = I^2R_a/V \quad (2)$$

Where V is the volume of power lithium battery, m^3.

Lithium ion battery will produce a lot of heat in the working process. If the battery is not dissipated timely and effectively, it will not only seriously affect the working performance and working cycle of the battery, but also cause spontaneous combustion or explosion of the battery. To load the cooling system on the battery to improve the working environment temperature of the battery pack, we must first understand the thermal behavior of the battery. Using the simulation software can effectively simulate the thermal behavior and temperature rise of the battery. In

this paper, SolidWorks is used to establish the geometric model of the battery, and star CCM + is used to simulate and analyze the temperature field of the battery in the charge and discharge state. The main parameters of the battery are shown in Table 1.

Table 1. main performance parameters of lithium ion battery

battery type	soft pack lithium battery
nominal voltage/V	3.2
nominal capacity /Ah	10
internal resistance /mΩ	≈10
charging current /A	≤10
continuous discharge current /A	≤20
maximum discharge current /A	50
upper cut-off voltage /V	3.65±0.05
lower cut-off voltage /V	2.5
cycle life	≥2000
battery weight /g	275±5
size/mm	209×107×7.5

2.2 Battery Pack Modeling

Taking the soft packaged lithium battery for pure electric vehicle as the object for modeling, the modeling should not only truly reflect the heat dissipation of power single lithium battery, but also reasonably set the number of variables to simplify the subsequent calculation workload. The modeling is composed of 144 single cells, which are arranged in columns and rows, and the overall dimension of the single cell is 209 mm×107 mm×7.5 mm. The external dimension and shape of the model are consistent. There are three air inlet and outlet openings with the same size and shape. The spacing between modules and between modules and the inner wall of the box is 10 mm. The power lithium battery pack with two arrangement modes of column and row is meshed by ICEM software, and the fluid area grid is encrypted to generate unstructured grid. The geometric model of the generated grid is shown in Figure 1. The overall grid model of each power lithium battery pack has about 1.5 million grid units. Unsteady state calculation is carried out, and standard turbulence model is selected. In the treatment of wall function, the standard wall function with wall boundary conditions is provided by logarithmic correction method. The computational domain is divided into air fluid domain and battery solid domain. The heat transfer mode between battery surface and air is coupled heat transfer. The heating power of power lithium battery changes with working conditions. Convective heat transfer is conducted on the external surface of the box, and the convective heat transfer coefficient is 5 $W/(m^2 \cdot K)$; SIMPLE algorithm is selected for the coupled mode of pressure and velocity; The second-order upwind scheme is used for the discretization of momentum, energy and pressure equations; The number of iteration step is 5000.

To establish an effective battery thermal management system, it is necessary to understand the internal temperature distribution of the battery pack. Through simulation analysis, we can roughly understand the temperature field distribution in the battery pack, and then optimize the structure of the battery pack according to the analysis results, so as to gradually establish an effective battery pack heat dissipation system. The battery pack contains 12 battery modules, and three fans are used to extract air. The geometric modeling of the battery pack is carried out through SolidWorks. The model is shown in Figure 1.

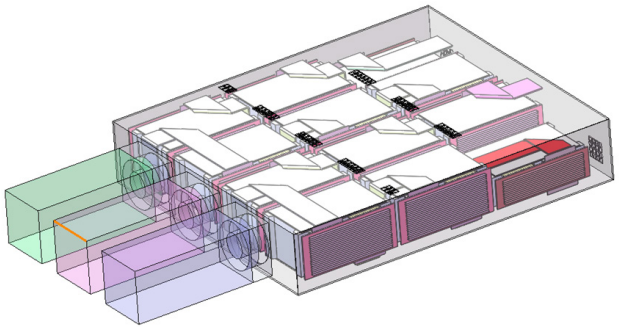


Figure 1. geometric model of battery pack

2.3 Battery Pack Simulation

When using star CCM + software for simulation calculation, the following assumptions are put forward for the whole simulation model: in the flow field inside the battery pack, the fluid is regarded as an incompressible ideal fluid without considering gravity and buoyancy; there is no relative sliding between the air and the battery and the inner wall of the pack; the inertial force of the fluid is ignored and the boundary pressure is zero, and ignore the thermal deformation of the whole system; the lithium battery is set as a constant heating source, and the air inlet is uniform air inlet conditions; radiation heat dissipation is not considered for the whole battery pack; it is assumed that the density and specific heat capacity of the single cell are constant; in the same direction, the thermal conductivity of the battery is not affected by SOC and temperature; when the battery is charged and discharged, the internal current density of the battery is uniform. See Table 2 for physical parameters of battery pack and Table 3 for fan parameters.

Table 2. material parameters of each part of the model

material	density kg/m^3	specific heat capacity $J/(kg*K)$	thermal conductivity $W/(m*K)$
aluminum alloy	913	2710	201
foamed silica gel	820	324	0.04
EVA foam	850	101	0.085
ABS+PC	1150	1300	0.24
coolant	1062	3305	0.418
battery cell	1933	1080	axial 0.66, radial 22.3
air	1.279	1006	0.024

Table 3. the parameters of fan system parameters

wind pressure (Pa)	375	250	187.5	150	125	0	speed (rpm)	size(mm)
air quantity (m/s)	0	0.02359	0.004719	0.07079	0.09439	0.11798	5000	140×140×51

2.4 Governing Equations of Computational Fluid Dynamics

In the process of fluid flow, three conservation laws are observed: the law of mass conservation, the law of momentum conservation and the law of energy conservation. In computational fluid dynamics [5,6], there should be: mass conservation equation, momentum conservation equation and energy conservation equation.

(1) Mass conservation equation

$$\frac{\partial \rho}{\partial t} + div(\rho U) = 0 \tag{3}$$

Where ρ is the fluid density; U is the velocity vector.

(2) Momentum conservation equation

$$\frac{\partial(\rho u)}{\partial t} + div(\rho u U) = div(\mu gradu) - \frac{\partial p}{\partial x} + S_u \tag{4}$$

$$\frac{\partial(\rho v)}{\partial t} + div(\rho v U) = div(\mu gradv) - \frac{\partial p}{\partial y} + S_v \tag{5}$$

$$\frac{\partial(\rho w)}{\partial t} + div(\rho w U) = div(\mu gradw) - \frac{\partial p}{\partial z} + S_w \tag{6}$$

Where ρ is the fluid density; u, v, w are the velocity components of velocity vector U in x, y, z directions respectively; μ is hydrodynamic viscosity; S_u, S_v, S_w are the generalized source term of the momentum conservation equation.

(3) Energy conservation equation

$$\frac{\partial(\rho T)}{\partial t} + div(\rho U T) = div\left(\frac{k}{C_p} grad T\right) + S_T \tag{7}$$

Where k is the heat transfer coefficient of the fluid; C_p is the specific heat capacity of the fluid; S_T is viscous dissipation term.

(4) Differential equation of heat conduction in battery

$$\rho C \frac{\partial T}{\partial t} = \lambda_x \frac{\partial^2 T}{\partial x^2} + \lambda_y \frac{\partial^2 T}{\partial y^2} + \lambda_z \frac{\partial^2 T}{\partial z^2} + q \tag{8}$$

Where ρ is the cell micro cell density; C is the specific heat capacity of micro cell of battery; λ is the thermal conductivity of battery micro element; q is the heat generation rate of battery micro element.

2.5 Thermal Management Simulation Strategy

The working condition of discharge: under the ambient temperature of 25 °C, the initial temperature of the system is 25 °C, and the total current of the battery pack is 2000 A, discharging for 4S (the heating power of cell is 19040 W; the heating power of collecting current aluminum bar is 2252.5 W; the heating power of welding aluminum bar is 43 W; the heating power of aluminum lug is 726.8 W, and the heating power of copper plate is 1805.2 W); then stop for 1S, and a total cycle is 5S; the discharging lasts for 10 cycles while the fan remains on.

The working condition of charge: keep the fan on, the total current of the battery pack is 150 A, charging for 900S (the heating power of cell is 816 W; the heating power of collecting current aluminum bar is 12.7 W; the heating power of welding aluminum bar is 0.24 W; the heating power of aluminum lug is 4.1 W, and the heating power of copper plate is 10.2 W).

3. Analysis of Simulation Results

Using the third-party post-processing software, the high and low temperature curves of each monomer of power lithium battery shown in Figure 7 are obtained. Among

them, 35 monitor is the maximum temperature curve of each monomer in column and row arrangement batteries, and 20 monitor is the minimum temperature curve of each monomer in column and row arrangement batteries. It can be seen from the curves in Figure 7 that the maximum temperature of monomers in column arrangement batteries is generally lower than that in row arrangement batteries. The maximum temperature change of each single cell in column arrangement batteries is relatively gentle, and the maximum temperature change of each single cell in row arrangement batteries is relatively rapid. The maximum temperature of 2 monitor to 11 monitor cells in column arrangement batteries decreases steadily, and the maximum temperature of 1 monitor and 12 monitor cells has a large temperature difference from their adjacent cells, but within the allowable temperature difference range. In the row arrangement batteries, the single battery of 1 monitor to 26 monitor are set as group I, and the single battery of 27 monitor to 46 monitor are set as group II. In each group of row arrangement batteries, the maximum temperature of each single cells presents the same arch distribution law, that is, the maximum temperature of 1 monitor to 26 monitor single cells presents a symmetrical distribution law. The maximum temperatures of 1 monitor and 6 monitor cells are almost the same and lower than those of 2 monitor to 5 monitor cells, and the maximum temperatures of 3 monitor and 4 monitor cells are slightly higher than those of 2 monitor and 5 monitor cells; Similarly, group II composed of 27 to 46 monitor single cells presents the same maximum temperature law. From the overall analysis of group I and group II, the maximum temperature of the single cell of group I is about 2.5 °C higher than that of the corresponding single cell of group II. According to the curve in Figure 7, the distribution law of the lowest temperature of each monomer in the two arrangement batteries of column and row is consistent with the distribution law of the highest temperature of each monomer in the two arrangement batteries of column and row. The maximum and minimum temperature curves of each monomer in column arrangement batteries are better than those in row arrangement batteries. That is, the column arrangement batteries are better in terms of maximum and minimum temperature. It can be seen from the temperature curve of each cell in the column arrangement batteries that the temperature difference between 1 monitor and 12 monitor cells is small, and the temperature difference between 2 to 11 monitor cells are large. In the column arrangement batteries, the temperature difference of 2 monitor single battery is the largest. It can be seen from the temperature curve of each cell in the row arrangement batteries that the temperature difference of each cell in group I and group II also presents an arch distribution law. The temperature difference of the single cells of group I is about 1 °C higher than that of the corresponding single cells of group II. In the row arrangement batteries, the temperature difference of 4 monitor single cells in the middle of group I is the largest.

The air cooling effect of heat dissipation of power lithium battery is closely related to the surface of single battery and the contact area of cold air. The single battery with large contact area between the column arrangement batteries and cold air are 1 monitor and 12 monitor, so they have good heat dissipation effect, low temperature and small temperature difference; In the row arrangement batteries, the single battery with large contact area with cold air are 1 monitor, 6 monitor, 7 monitor and 12 monitor, so they have good heat dissipation effect, low temperature and small temperature difference. The column arrangement batteries have good correlation between individual cells and small temperature change between cells, which is more conducive to ensure the temperature balance between individual cells.

The first discharge and charging cycle is completed, as shown in Figure 2. The maximum temperature of probe points is about 34.3 °C, and the minimum temperature of probe points is 30 °C, and the maximum temperature difference is 4.3 °C. The second discharge and charging cycle is completed, as shown in Figure 3. The maximum temperature of probe points is about 38.7 °C, and the minimum temperature of probe points is 31.7 °C, and the maximum temperature difference is 7 °C. The third discharge and charging cycle is completed, as shown in Figure 4. The maximum temperature of probe points is about 40.6 °C, and the minimum temperature of probe points is 32.4 °C, and the maximum temperature difference is 8.2 °C. The fourth discharge and charging cycle is completed, as shown in Figure 5. The maximum temperature of probe points is about 41.4 °C, and the minimum temperature of probe points is 32.6 °C, and the maximum temperature difference is 8.8 °C. The fifth discharge and charging cycle is completed, as shown in Figure 6. The maximum temperature of probe points is about 41.8 °C, and the minimum temperature of probe points is 32.7 °C, and the maximum temperature difference is 9.1 °C. During the whole working condition, as shown in Figure 7, the maximum temperature of all arranged probe points is 61.6 °C, and the maximum temperature difference is 9.1 °C, and the total time is 4750S.

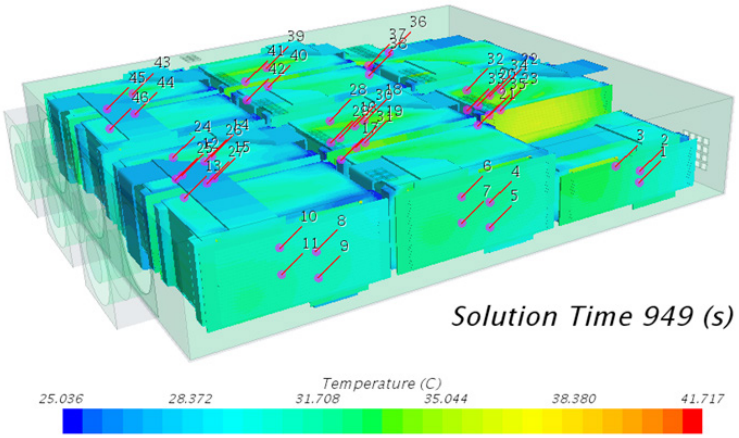


Figure 2. temperature distribution after the first discharge and charging cycle

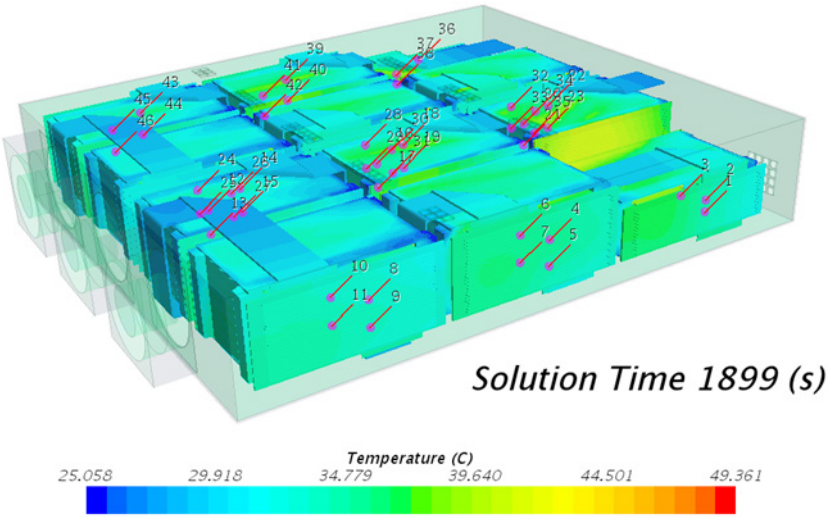


Figure 3. temperature distribution after the second discharge and charging cycle

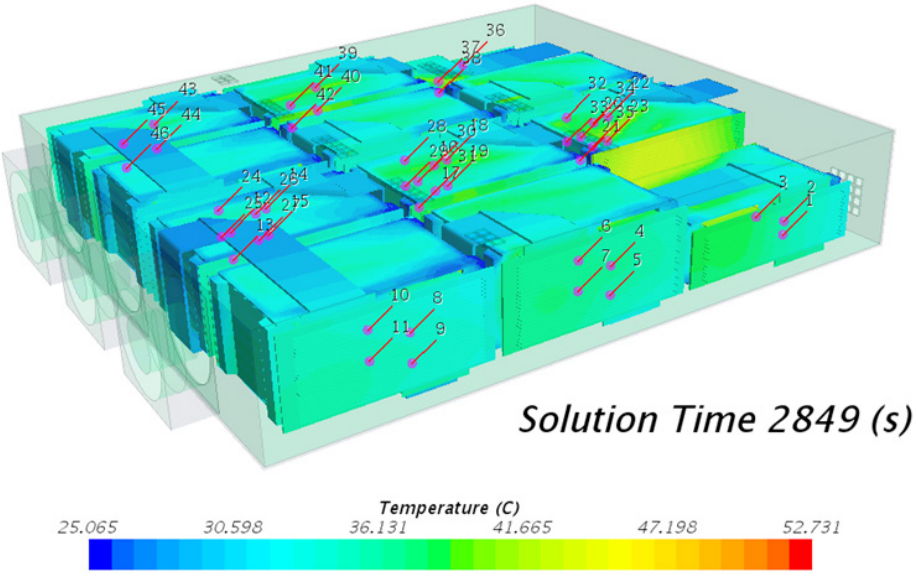


Figure 4. temperature distribution after the third discharge and charging cycle

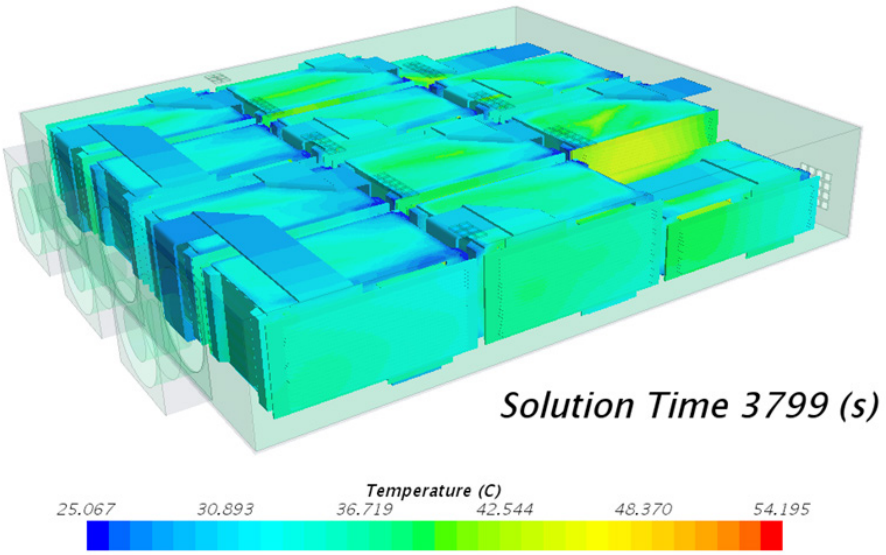


Figure 5. temperature distribution after the fourth discharge and charging cycle

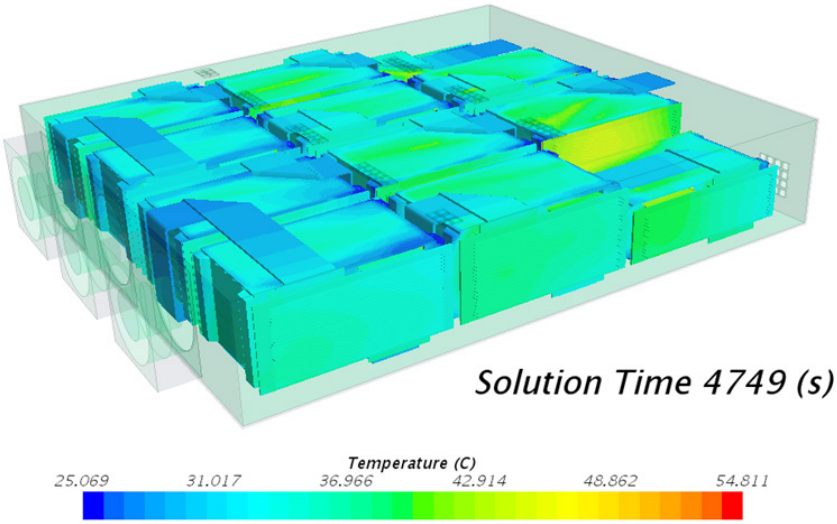


Figure 6. temperature distribution after the fifth discharge and charging cycle

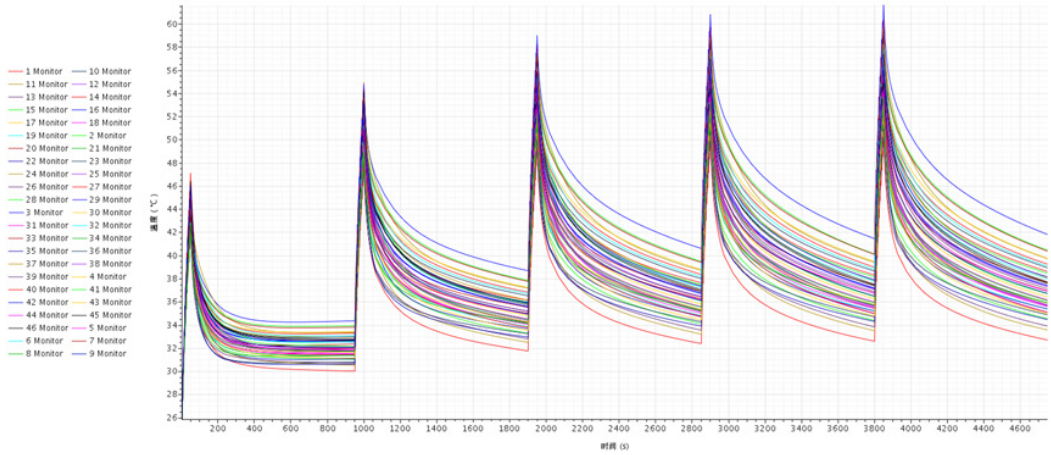


Figure 7. temperature variation curve of probe points with time

4. Conclusions

In order to optimize the heat dissipation system of electric bus power battery, the overall temperature distribution of the battery pack is understood through modeling and simulation of the battery pack, and the temperature difference and the maximum temperature are obtained. The conclusions are as follows:

(1) Through the simulation technology, the effectiveness of the thermal management control strategy of the air cooled system is verified, which can meet the heat dissipation requirements of the battery pack and prevent the thermal runaway of the soft packed lithium battery pack in the process of charge and discharge.

(2) When the battery pack is in the environment of 25 °C, the maximum temperature of the cooling system can be lower than 65 °C during the whole working condition, and the maximum temperature difference between all single batteries is within 10 °C.

Conflicts of Interest

The author declares that they have no conflicts of interest to report regarding the present study.

References

[1] Deng, Y., Yuan, Y., Zhang, X., 2015. An introduction of the application prospect of large capacity lithium battery in distributed energy storage system. Modern Machinery. (06), 83-86.

[2] Jarrett, A., Kim, I.Y., 2011. Design optimization of electric vehicle battery cooling plates for thermal performance. Journal of Power sources. 196(23), 10359-10368.

[3] Lei, Zh.G., Zhang, Ch.N., Lei, X.G., 2015. Research on thermal characteristics and thermal model of EVs lithium-ion battery. Advanced Technology of Electrical Engineering and Energy. 34(12), 59-63.

[4] Lu, Z., Meng, X.Z., Well, C., 2016. Thermal management of densely packed EV battery with forced air cooling strategies. Energy Procedia. 88, 682-688.

[5] Zhang, X., Wang, T., Xu, H.G., 2019. Simulation analysis of temperature of square power lithium-ion battery based on parallel air-cooling. Chinese Journal of Power Sources. 43(3), 426-428.

[6] Du, M.H., Zheng, X.W., Jiang, Zh.W., 2018. Analysis of influencing factors on heat dissipation performance on liquid-cooled of electric vehicle battery module. Guangdong Chemical Industry. 45(16), 48-50.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Electronic & Information Systems
https://ojs.bilpublishing.com/index.php/jeis

ARTICLE

3D Reconstruction of Fruit Shape based on Vision and Edge Sections

Nasr Abdalmanan Nasr Ali[1] Kamarulzaman Kamarudin[1*] Chee Kiang Lam[1] Muhamad Safwan Muhamad Azmi[2] Abdul Halim Ismail[1] Norasmadi Abdul Rahim[1] Wan Mohd Nooriman Wan Yahya[1] Goh Kheng Sneah[3] Moey Lip Seng[3] Teoh Phaik Hai[3] Ong Thean Lye[3] Noor Zafira Noor Hasnan[4]

1. Faculty of Electrical Engineering Technology, Universiti Malaysia Perlis, Kampus Alam Pauh Putra, Arau, Perlis, 02600, Malaysia
2. Faculty of Mechanical Engineering Technology, Universiti Malaysia Perlis, Kampus Alam Pauh Putra, Arau, Perlis, 02600, Malaysia
3. Walta Engineering Sdn. Bhd., Prai, Pulau Pinang, 13600, Malaysia
4. Department of Process and Food Engineering, Faculty of Engineering, Universiti Putra Malaysia, UPM Serdang, Selangor, 43400, Malaysia

ARTICLE INFO

Article history
Received: 1 April 2022
Accepted: 28 April 2022
Published Online: 13 May 2022

Keywords:
3D Reconstruction
Machine vision
Fruit processing

ABSTRACT

The fruit industry has been known as one of the largest businesses in Malaysia, where most of the fruits pass through the peeling process well in advance before the final product as juice in a bottle or slices in a can. The current industrial fruit peeling techniques are passive and inefficient by cutting parts of the pulp of the fruit with peels leading to losses. To avoid this issue, a multi-axis CNC fruit peeler can be used to precisely peel the outer layer with the guidance of a 3D virtual model of fruit. In this work, a new cost-effective method of 3D image reconstruction was developed to convert 36 fruit images captured by a normal RGB camera to a 3D model by capturing a single image every 10 degrees of fruit rotation along a fixed axis. The point cloud data extracted with edge detection were passed to Blender 3D software for meshing in different approaches. The vertical link frame meshing method developed in this research proved a qualitative similarity between the output result and the scanned fruit in a processing time of less than 50 seconds.

1. Introduction

Malaysia is one of the world's leading exporters of tropical fruits. Malaysia, as the world's largest producer of durian, mangosteen, and starfruit, produced 1.49 million metric tonnes in 2017 and exported roughly 268,400 metric tonnes [1]. Fruits were the most often purchased organic

*Corresponding Author:
Kamarulzaman Kamarudin,
Faculty of Electrical Engineering Technology, Universiti Malaysia Perlis, Kampus Alam Pauh Putra, Arau, Perlis, 02600, Malaysia;
Email: kamarulzaman@unimap.edu.my

DOI: https://doi.org/10.30564/jeisr.v4i1.4585

food by Malaysian consumers, according to a survey done by Wong & Aini in Klang Valley [2]. Therefore, fruits are progressively becoming a significant part of Malaysia's agricultural production. Stripping is one of the post-harvest operations used to prepare horticulture crops and tubers for processing, and peeling is an important element of the food preparation process during the early phases of food processing. Reducing peeling loss is one of the most important objectives in the fruit industry. Therefore many studies have been conducted in this particular field to improve fruit peeling machines [3]. In this research an approach of utilizing machine vision and image processing was introduced in the pre-peeling process to optimize peeling quality by digitally reconstructing a 3D model of the real fruit to guide a CNC peeler. 3D image reconstruction is the process to convert a series or a single 2D image to a 3D model. Many different techniques were introduced to perform this task, nevertheless, they all share the same concept of staging from image acquisition to image reconstruction [4].

3D Image Reconstruction Methods

Laser triangulation scanning for 3D image reconstruction is a setup of a single fixed camera with low exposure settings and a linear (vertical line) laser is usually fixed in tangent to the camera circumference towards the object in the centre. The object is rotatable on a perpendicular axis with respect to the setup plane. The system's concept is to measure the object in 3D space by optically measuring the distortion of the laser line casted on the object. Due to its geometry, the object needs to be rotated in a number of degrees and capture multiple scans to accurately get the shape of the object. However, this process is relatively time consuming, but the time could be minimized by increasing the number of laser modules within the range of the camera view to capture more geometry data in one rotation [5].

An advanced method of optical laser 3D reconstruction is based on Structured Light 3D scanning. Instead of using laser beams, the system utilises a light projector fixed next to the camera. The light projector will cast a series of high contrast light stripes patterns on the object and the processing part is to create a point cloud data based on the distortion of the light pattern casted on the object geometry captured by the camera [6]. Zhiping Xie performed a 3D image reconstruction of the Rosa Roxburghii fruit using structured light scanning method, where the point cloud processing algorithm developed achieved a volume error of 1.06% of the original fruit [7].

Another approach in 3D reconstruction field is using time-of-flight based RGB-D sensor to capture the depth information of a 2D scene. RGB-D camera consists of normal RGB camera and a depth sensor, where the depth sensor comprises of two major components: emitter and a receiver. The emitter blasts an infrared laser beam that hit the object and reflects back to the infrared receiver. Based on the delay time between emitting and receiving process, it is possible to calculate the distance between the sensor and the object acknowledging the fixed speed of light is $3\times10^8\ m/s$. This process of emitting, receiving and calculating is to be done rapidly for each pixel of the RGB camera register. Therefore the overall system returns the data of Red, Green, Blue, and Depth for each pixel [8]. The combination of RGB camera and depth sensor allow the system to scan an object's geometrical data along with texture and colour data [9]. Satoshi Yamamoto et al., attempted to reconstruct 3D images of an apple fruit using Kinect RGB-D sensor [10]. However, such methods are relatively complex to compute or process, and the cost of infrared pattern sensors, light structure 3D scanners and laser scanners are relatively high compared to only optical solutions. Therefore Mitchell J. Feldmann approach a low-cost 3D reconstruction with stereo vision system, which is a setup of two RGB cameras with a fixed distance in between to extract depth information with aid of trigonometry based on the object optical features [11].

Feldmann utilised a multi-view stereo method to scan fruits by capturing multiple images of the fruit from different angles with overlapping and created a point cloud by extracting the features of the images. They successfully matched the overlapped features points to be measured and obtained in 3D space [12]. An advanced technique of stereo vision is Photogrammetry, which is the method of three-dimensional estimation and measurement of an object in space by capturing a series of RGB or Greyscale images of the object from various angles [13]. The camera or multiple cameras are spherically moved around the object and the processing part is responsible for collecting the features points of intersecting between the images sequence. Thus, able to measure the position of the camera at every shot relative to the object and estimate the point cloud in space. This method not only capture the geometrical information of the object but also carries the object texture information [14], however, the scanned object surface is required to have a relatively rough texture with various features patterns. Nevertheless if the object texture is transparent, highly reflective or shiny, it would lead to failing the process of images stitching due to lack of visual features [15]. Another factor of photogrammetry precision is environment illumination since the overall method is completely depends on optical sensory only [13]. An attempt of strawberry fruit 3D measuring system was conducted by Nobuo Kochi et al., utilizing photogrammetry

method. A three-camera system was arranged vertically to obtain levelled view, above levelled view and below levelled view. The strawberry fruit is mounted on a rotational disc with a solid blue background colour. The overall process of image aquation, image processing and 3D modelling required 90 minutes to scan a single strawberry fruit with a matching error of 0.6 mm or less in 90% of the trials [16]. Table 1 compares the previous works of fruit 3D reconstruction. The key characteristics are the system cost and the complexity of the processing method.

This work proposes a method for 3D reconstruction of fruits based on edges sections with only optical sensing. A single RGB camera was used to extract the fruit geometry features via edge detection and convert it to point cloud data in three-dimensional space. The point cloud data were processed in Blender software and the results were evaluated in terms of the shape of the reconstructed 3D image.

2. Methods

Started by setting up the fruit on a rotating axis driven by a stepper motor as foreground, while the background is a solid colour plane, an RGB camera perpendicularly fixed to the axis is used to acquire the raw data set, which is a total of 36 images of the fruit taken from every 10 degrees of axis rotation. The reason of using a single RGB camera is to reduce the setup costs and complexity from the previous methods.

The current goal is to mask the fruit out from the background since the background is a solid chroma key colour. The alternative is to mask the background and then invert the mask values, however even though the background is in a single colour, the shadows and environment lightings will create a slight variation in colour hue and saturation which is very complex to process in RGB colour format. To begin the process, the images are converted from RGB colour format to HSV colour format. In RGB colour format every single pixel in the image is to be represented as a combination of (Red, Green and Blue) while in HSV colour format a single pixel is to be represented via three components Hue, Saturation and Value [17], this representation eases the work by clustering all Hues colours in one dimension instead of three dimensions, therefore selecting the range of the colour mask is less complex.

Where, $H = \cos^{-1}\left[\frac{0.5\,[\,(R-G)+(R-B)]}{\sqrt{(R-G)^2+(R-B)(G-B)}}\right]$, $S = 1 - \frac{\min(R+G+B)}{V}$, and $V = \frac{R+G+B}{3}$.

The mask result is representing the separation of the fruit in the foreground and the image background. Since the fruit is rotating on axis, there is no need of using the full image and only one half is enough. There is no significant difference between the top or bottom half of the image since the axes are centred and the fruit is rotating. In order to define the outer contour of the mask, a method of contrast detection is used, where a weighted 3 by 3 kernel mask is used for the convolution of the binary image. This process is performed to detect the pixels that has abrupt changes in intensity with respect to its 8-neighbours, defined as an edge pixel. The x and y image coordinates of edge pixels are then stored in a variable.

To represent the edge pixels as a point cloud in three-dimensional space, a method of double conversion is used. The first step is to convert the edge pixels coordinate system from (x, y) to (r, θ, z) also known as cylindrical coordinates system, where a point in space is to be represented by three components (i.e., r radius from axis line to the point, θ is the angle of vector according to the axis and z is the elevation of the point).

Firstly, the range of z from z_1 to z_2 is determined, where

Table 1. Fruit 3D reconstruction prior approaches summary

Author	Sensory	Sensing method	Reconstruction technique	Findings
Zhiping Xie	3D laser scanner	Structured Light Scanning	Point cloud processing	The results have high accuracy (98.94%). The sensor is relatively costive.
Satoshi Yamamoto et al	Kinect RGB-D camera	Time of Flight	Point cloud processing	The setup cost is good in value. Relatively complex processing due to sensor accuracy.
Mitchell J. Feldmann	RGB cameras	Stereo Vision	Point cloud via image segmentation	Low-cost system. Relatively lower results accuracy. To enhance the accuracy additional cameras could be added to the system leading to a cost increase.
Nobuo Kochi et al	RGB cameras	Photogrammetry	Point cloud via features extractions	High step cost due to usage of multiple DSLR cameras. High accuracy results. Relatively complex/ slow processing.

z_1 could be defined as the x coordinate of the first point of the edge, and $z_2$is the x coordinate of the last point of the edge. Then to determine the r value which is the vertical distance between the edge point and the axis, the absolute value of edge pixel (y component) is subtracted by axis (y component).

$$r = |EP[1] - axis[1]|$$

The y-axis component reference is equal to the y coordinate of the edge pixel pair that has the maximum y value in the list variable. Finally, angle θ is determined, which is equal to the angle of the axis in the current image. After establishing all the previous rules to calculate r, θ, and z components of each edge pixel, the data is re-registered as a group in a variable list to be called a section.

The next step is to convert all sections points from cylindrical coordinates system (r, θ, z) to cartesian coordinates system (x, y, z)

$$x = r\ \cos\theta\,,\quad y = r\ \sin\theta$$

The next procedure is to call the data, section by section in Blender software, where in each call, every point in the section is being plotted in space. Geometrical link is established between every subsequent point until all points in the section are linked (i.e., 1 to n points). The result of this process is a frame of connected point for each section as shown in Figure 1. The reason of connecting the relative points together vertically in each section is to aid the automated meshing process, where it generates a geometrical plane over the points and the linking lines guiding the algorithm to define the nearest shape. Then the observation method was used to verify the algorithm by observing the output image.

3. Results

The fruit in Figure 2 below is used to test the method. After the image processing operations were applied and all the sections points have been extracted, several meshing techniques were applied to obtain the 3D model. The first approach was by calling all the sections data at one time in Blender and directly generate the mesh using the python script with Blender to run the faces generator command. The faces generation algorithm in blender is a function that generates a geometrical plane that passes through three or more points in the point cloud object. Each point in the point cloud has a unique id in the memory, however when all the points are called at once, all the points will share the same id as one object. Therefore, the face generation function will attempt to randomly generate faces passed through the points leading to a random meshing as illustrated in Figure 3.

The second attempt was to call all the sections at once,

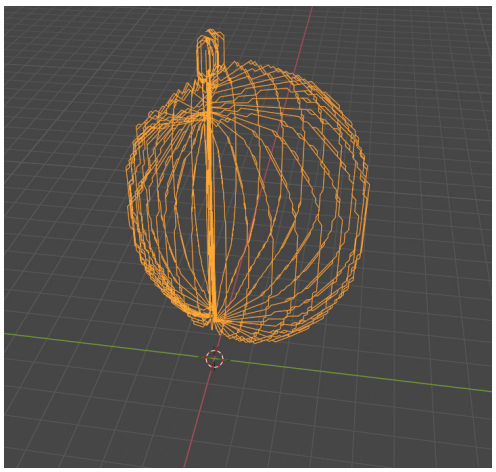


Figure 1. Framing process.

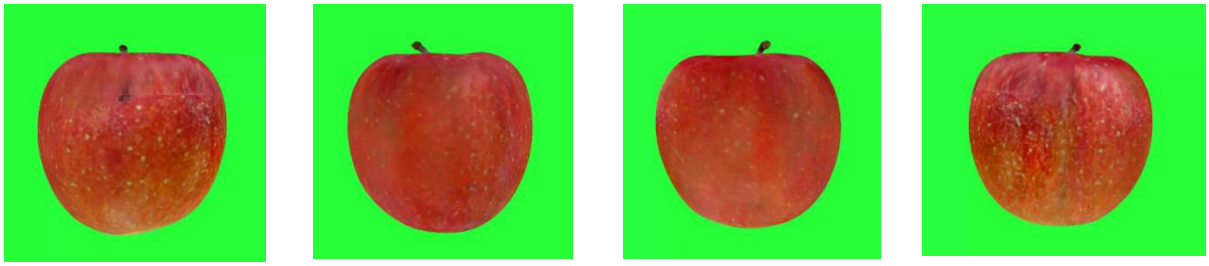
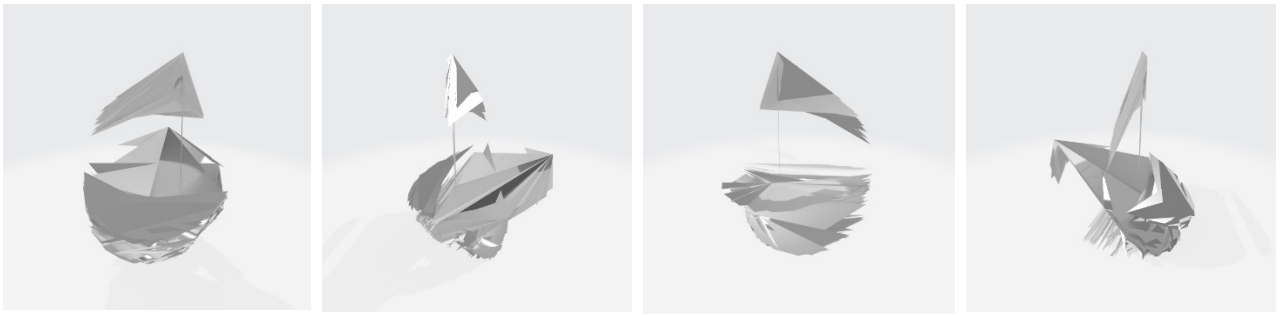


Figure 2. Apple fruit rotate around axis with solid colour background setup.



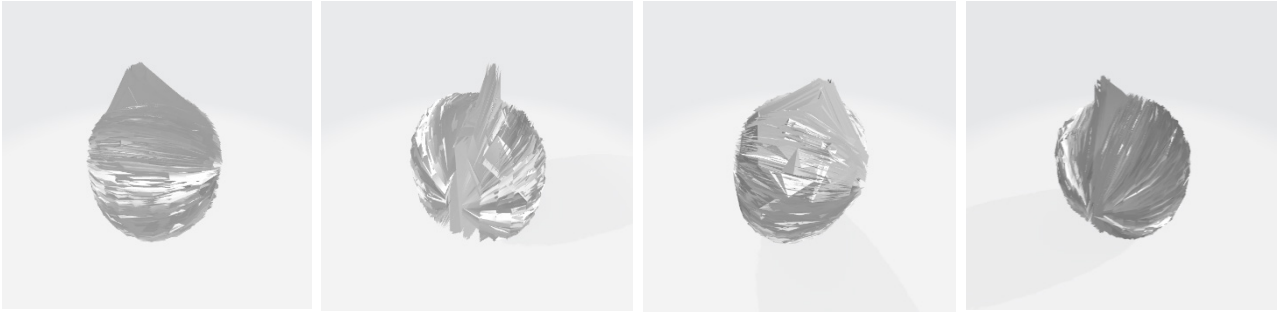
(a) **(b)** **(c)** **(d)**

Figure 3. Result of attempt 1 (a) front side view, (b) right side view, (c) back side view, (d) left side view.

followed by link framing and face generation operations. The framing operation was performed before filling faces in order to help to hold a structure that the faces will be constructed on. This way, the blender software would be guided with paths to perform face generation function (i.e., placement of the face shape, size, direction, and orientation). In this attempt, the points linking was complete but in a random way, means that every point is linked by a wire to all the others point which created a structured like a wool ball. Then the face generation algorithm worked on covering the structure with geometrical planes. However, the images rendered in Figure 4 are not similar in shape to the test sample.

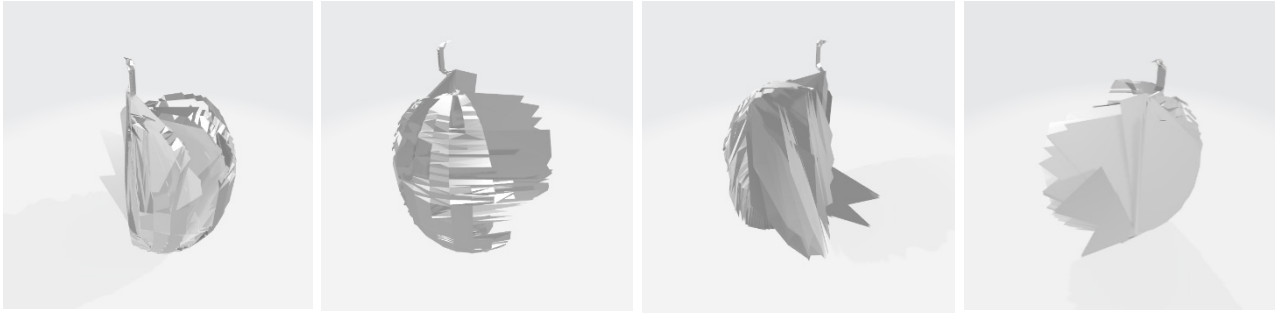
The next attempt was to call each section alone and operate a vertical frame linking algorithm, then eventually generate the faces. This means that every section will have a unique geometry id ranging from 0 to 35, where the total of all sections is 36. Instead of connecting all the points to each other, a method of connecting each section points only as group is used. This will function as a guide to the face generation algorithm to generate faces along the sections vertically instead of random. However due to the relatively large number of sections, the face generation function crashes at the middle of the process. The program was not able to continue generating the entire sections leaving a half empty frame without meshing as shown in Figure 5.

The final attempt was to call each section alone, followed by operating a vertical frame linking algorithm. The face generator was applied before calling the next section



(a) **(b)** **(c)** **(d)**

Figure 4. Result of attempt 2 (a) front side view, (b) right side view, (c) back side view, (d) left side view.



(a) **(b)** **(c)** **(d)**

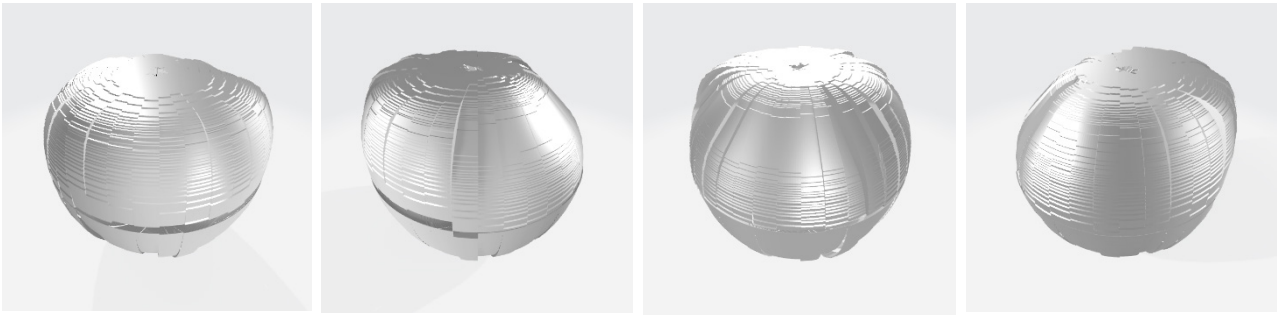
Figure 5. Result of attempt 3 (a) front side view, (b) right side view, (c) back side view, (d) left side view.

so that the face generation command shall deal with relatively small data at a time. This process took longer than usual due to operation of face generation command executed 36 times between calling the sections, however the result turned better than previous approaches where the generated mesh is relatively similar to the test object as shown in Figure 6.

Table 2 shows the summarized results of four attempts of meshing sequences in Blender software. The first three attempts showed distorted images of the input as the Blender software failed to build the correct surfaces without proper guides. However, the fourth attempt was successful as the output 3D image was less distorted and relatively similar to the shape of real fruit. However, the most computation time took among all four attempts is the fourth one.

4. Conclusions

To conclude, this work discussed the possibility of 3D fruit image reconstruction with one camera by the developed new method of sections slicing and meshing. Only qualitative analysis is included in the scope of this study. This algorithm is promising and have the possibility to reconstruct a 3D fruit model in Blender software with the tuneable parameters of frame generation and face generation, however the method proposed is limited to only axial symmetrical shaped fruits. In addition, it was found that, the face generator needs to be applied step by step for each section in order for the Blender software to generate more accurate 3D fruit reconstruction.



(a) **(b)** **(c)** **(d)**

Figure 6. Result of attempt 4 (a) front side view, (b) right side view, (c) back side view, (d) left side view.

Table 2. Overall results summary

Attempt	Sections calling	Framing	Face generation technique	Process time	Visual representation
First	All at once	No	Random / All at once	3 Seconds	Distorted
Second	All at once	Yes / Random	Along frame / All at once	7 Seconds	Distorted
Third	One at once	Yes / Vertical	Along frame / All at once	9 Seconds	Distorted
Fourth	One at once	Yes / Vertical	Along frame / One at once	44 Seconds	Less distorted

Conflict of Interest

There is no conflict of interest.

Acknowledgement

The authors would like to acknowledge the support from the University-Private Matching Fund (UniPRIMA) from the Research Management Centre, UniMAP and Walta Engineering Sdn. Bhd.

References

[1] Kamarubahrin, A.F., Haris, A., Mohd Daud, S.N., et al., 2020. Indigenous alternate fruit for dates: Critical review on the selection criteria for local prophetic fruits in Malaysia. Journal of Tropical Agriculture and Food Science. 48(2), 43-58.

[2] Wong, S.S., Aini, M.S., 2017. Factors influencing purchase intention of organic meat among consumers in Klang Valley, Malaysia. International Food Research Journal. 24(2), 767-778.

[3] Kohli, D., Champawat, P.S., Mudgal, V.D., et al., 2021. Advances in peeling techniques for fresh produce. Journal of Food Process Engineering. 44(10), e13826.

DOI: https://doi.org/10.1111/JFPE.13826

[4] Ham, H., Wesley, J., Hendra, H., 2019. Computer vision based 3D reconstruction: A review. International Journal of Electrical and Computer Engineering. 9(4), 2394-2402.
DOI: https://doi.org/10.11591/ijece.v9i4

[5] Wijayanto, I., Hadiyoso, S., Gunawan, T.M., 2018. Video Processing for Dual Laser 3D Scanner Prototype based on Cloud to Cloud Method. In 2018 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC). pp. 149-153. IEEE.
DOI: https://doi.org/10.1109/ICCEREC.2018.8712107

[6] Zhang, S., 2018. High-speed 3D shape measurement with structured light methods: A review. Optics and Lasers in Engineering. 106, 119-131.
DOI: https://doi.org/10.1016/j.optlaseng.2018.02.017

[7] Xie, Z., Lang, Y., Chen, L., 2021. Geometric Modeling of Rosa roxburghii Fruit Based on Three-Dimensional Point Cloud Reconstruction. Journal of Food Quality.
DOI: https://doi.org/10.1155/2021/9990499

[8] Zabatani, A., Surazhsky, V., Sperling, E., et al., 2019. Intel® realsense™ sr300 coded light depth camera. IEEE transactions on pattern analysis and machine intelligence. 42(10), 2333-2345.
DOI: https://doi.org/10.1109/TPAMI.2019.2915841

[9] Fu, Y., Yan, Q., Yang, L., et al., 2018. Texture mapping for 3d reconstruction with rgb-d sensor. In Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 4645-4653.
DOI: https://doi.org/10.1109/CVPR.2018.00488

[10] Yamamoto, S., Karkee, M., Kobayashi, Y., et al., 2018. 3D reconstruction of apple fruits using consumer-grade RGB-depth sensor. Engineering in Agriculture, Environment and Food. 11(4), 159-168.
DOI: https://doi.org/10.1016/J.EAEF.2018.02.005

[11] O'Riordan, A., Newe, T., Dooly, G., et al., 2018. Stereo vision sensing: Review of existing systems. In 2018 12th International Conference on Sensing Technology (ICST). pp. 178-184. IEEE.
DOI: https://doi.org/10.1109/ICSensT.2018.8603605

[12] Feldmann, M.J., Tabb, A., 2021. Cost-effective, high-throughput phenotyping system for 3D reconstruction of fruit form. The Plant Phenome Journal.
DOI: https://doi.org/10.1002/ppj2.20029

[13] Reljić, I., Dunđer, I., Seljan, S., 2019. Photogrammetric 3D scanning of physical objects: tools and workflow. TEM Journal. 8(2), 383.
DOI: https://doi.org/10.18421/TEM82-09

[14] Dostal, C., Yamafune, K., 2018. Photogrammetric texture mapping: A method for increasing the Fidelity of 3D models of cultural heritage materials. Journal of Archaeological Science: Reports. 18, 430-436.
DOI: https://doi.org/10.1016/j.jasrep.2018.01.024

[15] Li, J., Berglund, J., Auris, F., et al., 2018. Evaluation of Photogrammetry for Use in Industrial Production Systems. In 2018 IEEE 14th International Conference on Automation Science and Engineering (CASE). pp. 414-420. IEEE.
DOI: https://doi.org/10.1109/COASE.2018.8560496

[16] Kochi, N., Tanabata, T., Hayashi, A., et al., 2018. A 3D shape-measuring system for assessing strawberry fruits. International Journal of Automation Technology. 12(3), 395-404.
DOI: https://doi.org/10.20965/ijat.2018.p0395

[17] Oinosho, T., Kameyama, M., Taguchi, A., 2021. Color Conversion Formulae between RGB Color Space and HSI Color Space for Color Image Processing. In 2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS). pp. 1-2. IEEE.
DOI: https://doi.org/10.1109/ISPACS51563.2021.9651118

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Tel: +65 65881289
E-mail: contact@bilpublishing.com
Website: ojs.bilpublishing.com

2661-3204
01
9 772661 320223