iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4835

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Biometric Face-code DNA Colour Vector: A Unique Identity with Double Layer Encryption Approach

Kavya R[1]
Computer Science Department, KTU University

Abstract— Security issues assume an essential part of each association, as more noteworthy accessibility, what's more, access to data, thusly, infer that there is a more prominent need to ensure them. Numerous entrance control instruments, dialects, and frameworks have proposed over numerous years to address the issue of access to data inside frameworks. This undertaking builds up an encryption approach for the color vector, which goes about as an authenticity of the genuine user for the safe money exchanges. In the proposed framework, need two information sources, the face image of the user and a numerical information, to give an individual character through Information Fusion (IF) methods furthermore, biometric information encryption. In the wake of preparing, we get a hybrid fusion code and apply DNA cryptography to include an extra layer of security. At that point changed over to color vector were every user has the unique color vector for the safe exchange and is anything but difficult to deal with. The color vector is a novel way to deal with the guarantee secure environment for the digital money exchange and information transmission. This approach will give an unbreakable security and a twofold layer of encryption. By utilizing this created color vector, to a degree can keep away from attacks like brute force attack, replay attack, and Phishing attacks, and can ensure that the user is legitimate or not.

Keywords: - Encryption, Information Fusion, DNA Cryptography, Color Vector.

I. INTRODUCTION

Network security has turned out to be more vital to personal computer users, associations, and the military. With the appearance of the web, security turned into a noteworthy concern and the historical backdrop of security permits a superior comprehension of the development of security innovation. One of the principal imperative strides towards counteracting unapproved get to is client confirmation. With the ascent insecurity breaks and exchange fakes, there is an expanding interest for a higher security level in an individual distinguishing proof or check framework. Today human confirmation factors in three classifications, specifically

1) What you know, e.g password, secret, personal identification number (PIN);
2) What you have, such as token, smart card etc. and
3) What you are, biometrics for example.

The initial two traditional safety efforts are defenseless to security assaults and abuse. For instance, PINs and passwords can be shared among colleagues in a workgroup, which impressively debilitates the security level of the framework. In addition, secret word and PINs can be shared among clients of a framework or asset. Biometric highlights outperform these two strategies by offering a positive human identifier in view of a natural part of an individual. The principal preferred standpoint of biometrics is that it constructs acknowledgment in light of a natural part of an individual and the utilization of biometrics requires the individual to be confirmed to be physically present at the purpose of the verification. The acknowledgment procedure requests that the individual to be distinguished is physically present for the purpose of verification. This trademark reduces the constraint of utilizing a secret key or token that can't separate between an honest to goodness client and a gatecrasher. Furthermore, biometric highlights are non-transferable and non-shareable.

Secure correspondence is crucial to encourage the classified trade of data between any sender and recipient. These days, the web has turned into the media for all managing an account and electronic trade exchanges and it is extremely basic that the correspondence is made in a very secure way. Keeping in mind the end goal to take into account these security necessities, a lot of methods and frameworks created in the numerical cryptography for encoding and deciphering the plain content. Nonetheless, these methods are beaten utilizing DNA cryptography procedures and techniques. The DNA cryptography is a rising field in the zone of DNA registering research. DNA cryptography assumes major a part of cutting-edge security. Deoxyribo Nucleic Acid or DNA is the hereditary material in people and relatively every another life form. A similar DNA is contained in almost every cell in a man body. Nowadays security is a big matter of concern. With the rise in security breaches and transaction frauds, there is an increasing demand for a higher security level in a personal identification or verification system. The proposed work build an effective encryption approach for proving the authentication of the user and the real identity of the owner for each cryptocurrency transaction. A possible application of this technique of data fusion is associated with the authentication of a person, for example, to guarantee

the access to private areas, to classified and confidential documents, privileges to activate critic, military or defensive infrastructures, etc.

II. BACKGROUND

The Information Fusion is yet a rising field of research [3]. Data Fusion field is normally seen as a multidisciplinary examine field including particular research zones (i.e. Information Mining, Knowledge Discovery, Artificial Intelligence, etc.)[5] depicted themselves by a multidisciplinary and by specific research bunches [6]. As the starting stage, use the framework proposed in [1]. This methodology has been subjected to fitting extensions. The strategy as of now proposed produces unmistakable verification codes to high security for affirmation measures [15].

Biometrics offers a characteristic and dependable answer for specific parts of personality administration by using completely robotized or semi-mechanized plans to perceive people in light of their organic attributes[9]. By utilizing biometrics, it is conceivable to set up a personality in view of your identity, as opposed to by what you have, for example, an ID card, or what you recall, for example, a secret key. In a few applications, biometrics might be utilized to supplement ID cards and passwords subsequently bestowing an extra level of security. Such a game plan is regularly called a double factor verification conspire [13].

Information Fusion field is usually viewed as a multidisciplinary investigate field including distinctive research . This strategy has been subjected to fitting expansions. The technique already proposed produces recognizable proof codes to high security for confirmation measures. While this approach consolidates Biometric code (Finger Code) and a numerical code in view of primality (RSA), to make a key encryption, by combining a numerical part, in view of primality (RSA Module), and an irregular number created by the fractal recipes[2]. As in [1], the development technique for the new code (key) created by the algorithm of fusion, will rely upon the private key of the RSA Algorithm. Encryption Approach Using Information Fusion Techniques Involving Prime Numbers what's more, Face Biometrics make an entrance key with exceptional attributes[2][3].

Gerardo Iovane fabricates an access key for the protected exchanges in the blockchain [1], two non-associated territories have been joined, Face Biometrics and Public-key Cryptography to give an individual personality through Information Fusion (IF) strategies and biometric information encryption. An inventive and unique algorithm has been produced by G. Iovane, L. Puccio, G. Lamponi and A. Amorosia, which is the combination activities amongst biometric and numerical information [2], that is a calculation of Hybrid Information Fusion, named BNIF (Biometric and Numerical Information Fusion), to utilize an advanced unique mark as a biometric segment, and the result of two prime numbers as a numerical component, that is the module in RSA calculation.

SIFT algorithm is one most element extraction calculation utilized as a part of PC vision to identify and depict the neighborhood highlights of the picture [11]. The calculation was licensed in Canada by the University of British Columbia and distributed by David Lowe in 1999. Applications incorporate question acknowledgment, mechanical mapping, and route, picture sewing, 3D displaying, motion acknowledgment, video following, singular recognizable proof of untamed life and match moving.

Part of procedures and frameworks has been produced in light of secluded number juggling cryptography for encryption and decoding. Be that as it may, these strategies are broken utilizing DNA cryptography systems and techniques. DNA Cryptography is another natural cryptographic field that has risen up out of the exploration of DNA registering [17][18]. A few calculations that are accessible in DNA Cryptography have constraints in that despite everything they utilize particular math cryptography at a portion of their means or they are organic research facility explore based which isn't reasonable in the advanced registering condition. To beat this lacuna, Noorul Hussain UbaidurRahmana and Chithralekha Bala Murugan, portray a novel, secure, interesting and dynamic DNA based encryption and unscrambling calculation and give an examination of its execution.

III. BIOMETRIC FACECODE DNA COLOR VECTOR

This project develops encryption approach for Color vector, which acts as an identity of a legitimate user for the secure money transaction. The first capture the image of the user or user can upload the image and processing that images by SIFT algorithm to get the face code. The second input is the bit data, processing by RSA algorithm to form private key and module (product of two prime numbers) as a numerical vector. The hybrid fusion code can be formed from the face code, private key, and module vector. The hybrid face code is an access key, which is secured by adding the DNA cryptography and convert it into a unique color code. Each user has a unique color code for the secure exchange of digital money. DNA cryptography provides a good layer security layer, which does not give any hint about the plaintext.

A. System Architecture

Nowadays security is a big matter of concern. With the rise in security breaches and transaction frauds, there is an increasing demand for a higher security level in a personal identification or verification system. The proposed framework to build an effective encryption approach for proving the authentication of the user and the real identity of the owner for each cryptocurrency transaction. Figure.1 shows the system architecture; here use two inputs face image and bit data. First needed to capture the image of the real user or upload the face image, and converted into a face code. Through the SIFT algorithms extract the biometric features of the image which is used for the hybrid fusion code. Then you can get the correspondent of a face code, as a numerical vector. At that, time, input a bit data and processing by secure RSA algorithm to get the private key vector and a module vector. Then combine the face code and private key and module vector from bit data to form the hybrid face code by Face Information (FIF) algorithm. The

hybrid face code can likewise go about as an access key, moreover, include an additional layer of security by DNA cryptography and hybrid face code can be changed over into the color vector for the simplicity of use.

The hybrid face code is a novel solution, which can also be used within the trans-action of electronic currencies (block chain) but we apply DNA cryptography to add an additional layer of security to the face code. Therefore, it provides a good security layer, which does not give any hint about the plaintext. Then converted into color vector were each user has a unique color vector for the secure transaction and is easy to handle. The color vector is a novel approach to ensure a highly secure environment for the cryptocurrency transaction. This approach will provide an unbreakable security and a double layer of encryption. In the proposed system, build up an encryption approach for the color vector, which contains the users' biometric face attributes.

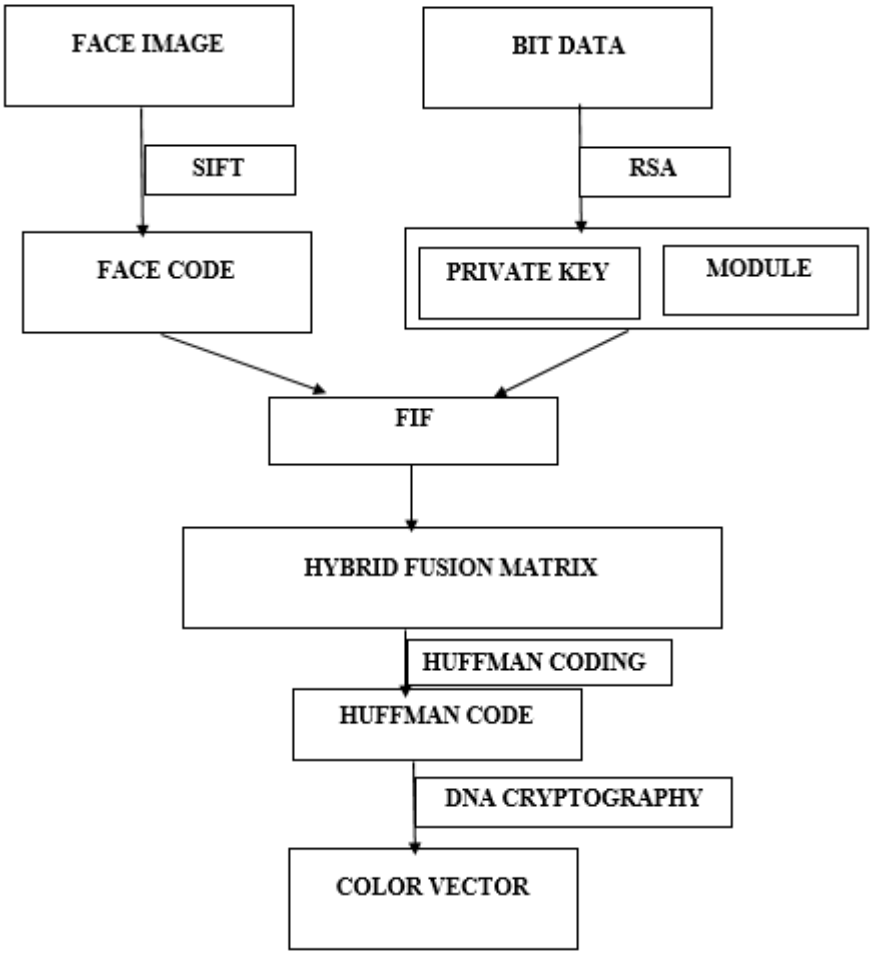


Fig 1: System Architecture.

Data Fusion (IF) is a generally present day inquire about the field: information originating from in excess of one source are at long last combined so as to get a super-data, where the richness of the details. In this framework, we join two data assets face image of the user and its information. The last yield color vector contains the users inherent, one of kind facial qualities, which are not the same as different clients. Biometric systems are increasingly important since they provide more reliable and efficient means of identity verifications. One of the first important steps towards preventing unauthorized access is user authentication. User authentication is the process of verifying a claimed identity.

B. Face Image Feature Extraction – SIFT

The system need two inputs, one is face image and other is bit information. The user can upload or capture the face image of the user. The corresponding face image can be converted into face code by SIFT algorithm. SIFT (Scale Invariant Feature Transform) algorithm, an algorithm in computer science to detect and describe the local features in an image [11]. SIFT algorithm is successful in feature matching research areas. The features extracted by SIFT are invariant to image scaling and rotation. Using SIFT algorithm generated face code as a numerical vector. The face code is used to generate the hybrid fusion code. The real advances utilized for the component extraction SIFT calculation are demonstrated as follows:

1) Constructing a scale space, this is the underlying readiness. You make inward portrayals of the first picture to guarantee scale invariance. This is finished by producing a "scale space".
2) LoG Approximation: The Laplacian of Gaussian is extraordinary for finding fascinating focuses (or key focuses) in a picture. Nevertheless, it is computationally costly. Therefore, cheat and estimated it utilizing the portrayal made before.
3) Finding key points: With the super quick estimation, we now attempt to discover key points. These are maxima and minima in the Difference of Gaussian picture we ascertain in stage 2.
4) Get free of the terrible key focuses: Edges and low complexity districts are awful key points. Disposing of these make the calculation proficient and strong. A system like the Harris Corner Detector is utilized here.
5) Assigning an introduction to the key points: An introduction is figured for each key point. Any further counts are done with respect to this introduction. This viable offsets the impact of introduction, making it pivot invariant.
6) Generate SIFT highlights: Finally, with scale and turn invariance set up, one more the portrayal is created. These aides particularly distinguish highlights. Let us say you have 50,000 highlights. With this portrayal, you can without much of a stretch distinguish the component you are searching for.

User image is uploaded at first, then by using SIFT algorithm, the user image is extracted into mark on image, which has marked all local features from the user image.

C. Bit Data - RSA

The second contribution to the framework is bit information; bit information can be handled by the RSA calculation. Utilizing RSA calculation to create the private key and module (product of two prime numbers) as the numerical vectors. The RSA algorithm is named after Ron Rivest, Adi Shamir, and Len Adleman, who invented it in 1977 [RIVE78].The RSA cryptosystem is the most widely used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. The user inputs a bit data, and then the RSA algorithm to get the private and module processes it. The module represents the product of two prime numbers used in the RSA calculation. .The private key and module vector as a numerical vectors.

The RSA algorithm is given below;:

1) Generate two large random primes, p and q
2) Compute n = pq and (phi) φ = (p-1)(q-1)
3) Choose an integer e, 1 < e < phi, such that
   gcd (e, phi) = 1.
4) Compute the secret exponent d, 1 < d < phi, such that e d ≡ 1 (mod phi).
5) The public key is (n, e) and the private key (d, n).

D. Hybrid Fusion Code – FIF

The FIF (Face Information Fusion) Algorithm is to join the face image of the user and a bit data to form a one of a kind unique vector [3]. In the accompanying, you can see the piece plot demonstrating a rundown of the principal periods of the framework, which makes the information combination. FIF algorithm used for the transformation of two vectors into one matrix, that is merge face code, module and private key vectors. The hybrid fusion vector can in like manner go about as an entrance key [8] [10].

To begin with, transfer the picture of the real user, and changed over into a face code. Through the SIFT calculation isolate the biometric features of the photo which is used for the hybrid fusion code. By then, you can get the writer of a face code, as a numerical vector. Around then, input a bit data and getting ready by secure RSA calculation to get the private key vector and a module vector. By then, merge the face code and private key and module vector from bit data to outline the hybrid fusion vector by Face Information Fusion (FIF) calculation [9].

The calculation of Face Information Fusion goes for getting a Fusion Key start from biometric and numerical information. A dire time of this calculation is the difference in two vectors into one vector. It is basic that this network is squared and that its demand depends upon the amount of the fragments of the two vectors [14]. To have this, it is imperative to take after these methods:

1) Be a, b € Z, two vectors, where a contains the biometric component and b the product of two prime numbers.
2) Be s € Z :
   s=m + n; where m and n are size of the biometric vector and module vector.
3) Be q € Z :
   q= [√ s] a whole number containing s root.
4) To reduce the size of two vectors by,
   nz1 = q-mod (m. q) and nz2 = q-mod (n. q).
5) The new size of the vectors is given by,
   m1 = m+nz1 and n1 =n+nz1.

6) In addition, divide each vector in blocks which will be the lines of the hybrid vector, a vector containing the two vectors inserted in a proper way,
nbloocc_a1 = m1/q and nbloocc_a1 = n1/q.

7) .Be: P ad = nz1 + nz2,

8) In order to insert the blocks is given by the private key; value of the first component of the private key defines the no of the blocks of the face code vector to be inserted into the hybrid vector and the second component of the private key define the no of blocks of the module vector to be inserted into the hybrid vector and so on.

9) Finally, the algorithm has to verify that the obtained matrix is really squared as,
PadTot = q2 − (m + n),
Diff = P ad – PadTot
Then, three cases can be distinguished:
Diff < 0 =⇒ addition of a line,
Diff = 0 =⇒ no added padding,
Diff > 0 =⇒ addition of a column.
The padding line or column to be added id created using the private key.

10) When you fabricate the squared Union U matrix, a post-result of grid U and permutation matrix P is done, henceforth you get a difference in sections. The private key of the cryptography of the calculation picks the permutation matrix. This framework, whose measurements are like the ones of matrix U, is formed consolidating six 3×3 frameworks of change, got from a similar grid:

11) At long last, you include the result of Union Matrix U and permutation P framework:
F= UP

12) Fusion F framework you acquire will be separated and organized along the lines to fabricate the yield V vector that is the Hybrid Face Code.

To decrease the length of the hybrid code vector for simple to deal with, utilize Huff-man coding to shape Huffman code. Huffman coding is a lossless information pressure calculation. The thought is to dole out variable length codes to enter characters; lengths of the relegated codes depend on the frequencies of relating characters. The successive character gets the littlest code and the slightest incessant character gets the biggest code.
Apply an extra layer of security by including DNA cryptography. Finally, the DNA code is changed over into the color vector.The DNA encoding arrangement can be changed over into Unicode, at that point, it is changed over to color vector for effortlessness of utilization. Information encryption system changes over information into a muddled arrangement in order to shield the data from outer intrusion. It is therefore helpful in guaranteeing the protection and security of the data exchanged or shared between the systems. Text pressure calculations can be utilized to conservative the content put away in the document and decrease the measure of the record. It lessens the utilization of assets, for example, hard plate space or transmission data transfer capacity. Here, we propose a shading coding plan that can be utilized for information encryption which speaks to content as shaded pieces by gathering together twofold bits and doling out them hues alongside Huffman encoding conspire which is utilized for lossless content pressure.

IV. CONCLUSION

The proposed system creates the color vector, which goes about as a character of the true blue client. Security issues expect a basic piece of every relationship, as more important availability and access to information, subsequently, gather that there is a more imperative need to guarantee them. Various passageway control parts, tongues, and systems have been proposed over various years to address the issues of access to information inside structures. This assignment makes encryption approach for Color vector, which goes about as an identity of a true blue customer for the secured money trade. To begin with getting the photo of the customer or customer can exchange the photo and taking care of that photos by SIFT figuring to get the face code. What's more, client inputs a bit information to get a private key vector and a module vector. The face code, private key vector, and module vector are joined to shape hybrid fusion code. The hybrid fusion vector is additionally an entrance key, which is secured by including the DNA cryptography and change it into an exceptional color vector. Every customer has an exceptional color vector for the safe secure exchange of automated money.

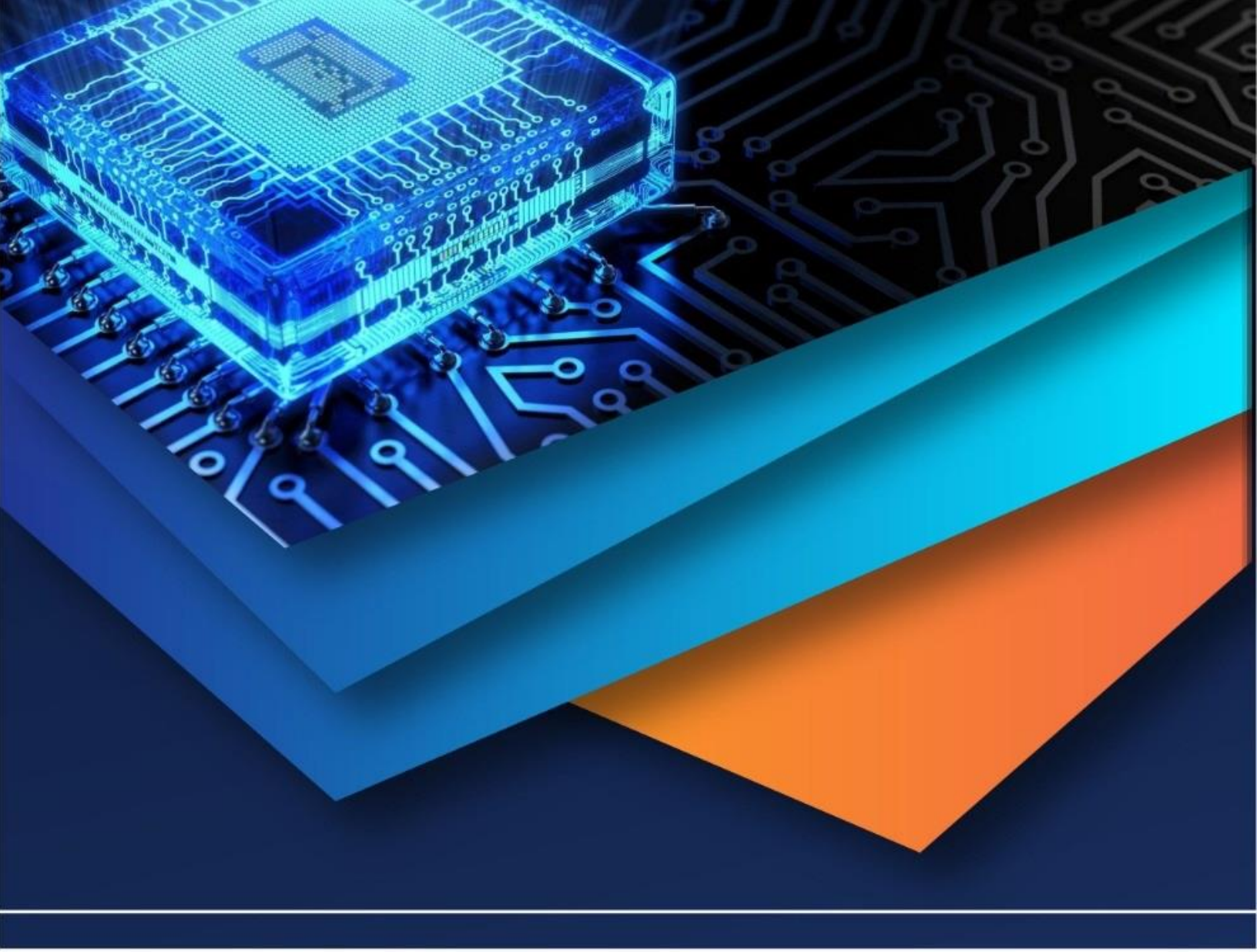
V. ACKNOWLEDGMENT

We would like to express our sincere gratitude to the teaching faculty at SJCET whose timely inputs and suggestions, helped in the completion of the project. We would also like to thank the Library and Computer Centre Departments of our college for allowing us to carry out our research. Finally, we are thankful for having been given this opportunity to learn something new about the world of technology.

REFERENCES

[1] Gerardo Iovane and Michele Nappi," An Encryption Approach Using Information Fusion Techniques Involving Prime Numbers and Face Biometrics", 2018
[2] G. Iovane, A. Amorosia, E. Benedetto G. Lamponi, "An Information Fusion approach based on prime numbers coming from RSA algorithm and Fractals for secure coding", 2015.
[3] Federico Castanedo, "A Review of Data Fusion Techniques", the Scientific World Journal, 2013.

[4] Jisha Nair.B.J, "A Review on Biometric Cryptosystems", Vol. 6 Issue 1 September 2015.
[5] B.V. Dasarathy, "Information fusion - what, where, why, when, and how?" Information Fusion, 2(2):75–76, 2001.
[6] F Chafia, C Salim and B Fraid, "Biometric crypto system for authentication", International Conference on Machine and Web Intelligence pp. 434 -438, 2010.
[7] R Sashank Singhvi , S.P. Venkatachalam , P.M.Kannan and V .Palanisamy , " Cryptography key generation using biometrics", International Conference on Control ,Automation, Communication and Energy conservation, pp. 1-6, 2009.
[8] Kavya R, "Survey on encryption approaches using information fusion with biometrics", International Journal of Advance Research, Ideas and Innovations in Technology, 2018.
[9] J. C. Zapata, C. M. Duque, Y. Rojas Idarraga, Miguel A Becerra, " Data Fusion Applied to Biometric Identification – A Review", pp.721-733, 2017.
[10] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification", IEEE transactions on pattern analysis and machine intelligence, pp. 1295–1307, 1997.
[11] M.Manzo, E.Sangineto, L.Cinque,and G.Iovane, " Face recognition using sift features and a region-based ranking", Journal of Discrete Mathematical Sciences and Cryptography, 2010.
[12] A. Lumini and L. Nanni., "An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers", Neuro computing, pp. 1706 – 1710, 2006.
[13] N. Poh and J. Korczak., "Hybrid biometric person authentication using face and voice features", pp. 348–353, 2001.
[14] A. Ross and A. Jain, "Information fusion in biometrics", pp. 2115 – 2125, 2003.
[15] F. Yang, B. Ma, Q. Wang, and D. Yao, "Information fusion of biometrics based-on fingerprint, hand-geometry and palm-print", pp. 247–252, 2007.
[16] Tushar Mandge, and Vijay Choudhary, "A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme", 2015.
[17] Aditya Gaitonde, "Color Coded Cryptography", Volume 3, Issue 7, July-2012.
[18] Devyani Patil , Vishakha , Akshaya Sanghavi and Aparna Bannore, "Cryptography based on Color Substitution", International Journal of Computer Applications, Volume 91, 2014.
[19] Anurag Roy and Asoke Nath, "DNA Encryption Algorithms: Scope and Challenges in Symmetric Key Cryptography", Issue 11, Volume 32, 2018.
[20] Noorul Hussain UbaidurRahmana, Chithralekha Balamuruganb and Rajapandian Mariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", International Conference on Information and Communication Technologies (ICICT), Pp.463 – 475, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY