Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-3 Issue-2, November 2023

Cryptographic Security Approach for Biometric Verification System

Akinribido C.T, Olabode O.O, Adetunmbi O.A, Adewumi Moradeke. Grace

Abstract ***This paper presents cryptography which is the science of encryption and decryption to protect fingerprint that can be transmitted from sender to receiver. This security approach (cryptography) can also be applicable to other biometric traits like face, iris, retina and palm print. The significant of this protective medium is to prevent intruders or attacker to easily perceive the presence of fingerprint images. The method that was utilized for implementation of this cryptographic security approach for fingerprint verification System was achieved through Elliptic Curve Cryptography and Hill Cipher Algorithm. An elliptic Curve Function was defined and its domain parameters were used to generate self invertible key matrix that was used for the encryption and decryption process of the biometric images (Fingerprint, Face and Ear) The security approach was also improved by ensuring that the decryption can only be done through secret key. After decryption, fingerprint verification was done by extracting and matching distinct feature (ridges) from template fingerprint and distinct feature from input fingerprint. The result obtained from demonstration of the cryptographic approach allows end users to load fingerprint image, encrypt it at sending end. At receiver end, end user can decrypt the fingerprint image. Image enhancement was later done before authentication through extraction and matching of distinct features. This model will prevent destruction and manipulation of stored fingerprint image. Authentication can also be accomplished through biological traits instead of use of password that can be stolen or transferred to relative.***

Keyboard: Cryptography, Verification, Fingerprint, Pixel Value

I. INTRODUCTION

Cryptographic Security approach to Fingerprint Verification Model is the process of individual identification that involves coding of biometric traits to form secret and easily differentiated data. The system can be achieved through extraction and protection of distinct features from biological traits that can be captured in form of images. In this study, the cryptography fingerprint Model utilized fingerprints traits.

Manuscript received on 03 July 2023 | Revised Manuscript received on 07 November 2023 | Manuscript Accepted on 15 November 2023 | Manuscript published on 30 December 2023.
** Correspondence Author(s)*
Akinribido C.T*, Department of Computer Science, Federal University, Oye Ekiti. E-mail: comforttomiye@gmail.com, ORCID ID: 0009-0003-3379-6367
Olabode O.O, Department of Computer Science, Federal University of Technology, Akure. E-mail: oolabode@futa.edu.ng, ORCID ID: 0000-0001-9105-7405
Adetunmbi O.A, Department of Computer Science, Federal University of Technology, Akure. E-mail: aodetunmbi@futa.edu.ng, ORCID ID: 0000-0003-4608-5057
Adewumi Moradeke. Grace, Department of Computer Science, Bamidele Olumilua University of Education, Science and Technology, Ikere - Ekiti. E-mail: adewumi.moradeke@bouesti.edu.ng, ORCID ID: 0000-0002-5224-3202

© The Authors. Published by Lattice Science Publication (LSP). This is an open access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Fingerprint features can be extracted from a sample fingerprint images using Orientation features and Local Direction Pattern (Chaudhary *et al* , 2014, [3]) It is very essential to control and prevent attackers to easily detect and perceive biometric traits which can be transmitted for strict monitoring of access to activities and properties (Authentication purpose).

Cryptographic Security approach to fingerprint Verification Model revealed cryptography which is the science of security that entails encryption and decryption phase. Cryptography can involves text, image, video audio, graphics and other multimedia. (Quist-Aphetsi (2013), [6]) emphasized on encryption technique which was based on RGB pixel shuffling of M * N size image. This encryption method was utilized for encryption of selected human facial area in connection to abuse cases on broadcasting media. Most existing biometric system does not cater for security. Cryptographic Security approach to fingerprint Verification Model will protect and avoid destruction of biometric trait before and at the point of life check. This will prevent unforeseen circumstances during biometric trait authentication. Cryptography was utilized to secure and protect biometric traits (fingerprint) that can be captured and utilized for authentication purpose.

Cryptography is process of hiding content of a message either image or text. In this work, existence of captured fingerprint was hidden. This will not allow attackers to see and perceive the fingerprint image. Cryptography can help to hide biometric trait that are captured during registration till date of authentication or verification for life check. This is also important for security and protection of biometric data during transmission from sender to receiver.

Cryptographic Security approach to fingerprint Verification Model also entails fingerprint recognition where distinct features were extracted from captured fingerprint. The distinct features include fingerprint ridges and valley. Authentication or Verification of fingerprint were determined by matching distinct features from captured or input fingerprint with distinct features of template fingerprint. (Yuliang *et al.*, 2003, [11][16]) explained that authentication of captured fingerprint can be done by comparing and matching of minutiae or ridge features of input and template fingerprint. The uniqueness of fingerprint can be determined by the pattern of ridges and valleys as well as minutiae points (Afsar et al., 2004, [1]). Protection of this distinct minutiae feature especially fingerprint image were not taken into consideration. The existing biometric system does not take into consideration security and protection of biometric traits that are captured in form of image.

Another major problem in biometric system that should be taken into consideration is manipulation and destruction of biometric data like fingerprint and facial image.

A. Research Motivation

One of the motivations of cryptographic Security approach to Fingerprint Verification Model is use of biometric trait to overcome problem of password as password can be transferred while biometric traits cannot be transferred to anybody. Writing of password can also cause problem to security measures. The significant of biometric trait to identify an individual and gain access to properties and asset cannot be compared to other traditional method like key, password and signature. Passwords can be forgotten and key can be stolen. Signature can as well be forged.

Biometric trait is physiological trait that is unique for everybody. It cannot be transferred, forgotten or stolen. In banking sector, ATM passwords were requested by fraudster through communication media like phone call, phone text messages, internet banking, e-mail etc. Some ignorant customers sent their password via e-mail believing a message was from their bank to send ATM password. The mission of the fake message cannot be achieved if biometric traits like fingerprint and face that cannot be transferred are used for ATM authentication (Vivek *et al.*, 2011, [7]). Also, password written by staff in bank can be stolen as PIN number is sometime written in paper for customers. This written document can be stolen with ATM card by friends and family member to withdraw money. With advert of biometric, these stealing methods will be abolished.

II. RELATED WORK

A. [Quist-Aphetsi Kester] 2013 A Cryptographic Image Encryption Technigue for Facial-Bluring of Images

This paper proposed image encryption techniques that enable selected facial area to be encrypted or blurred for events relating to sensitive information like activism, abused cases and others on public broadcasting media and social networks.

Method: The facial- blurring of images was achieved based on RGB pixel shuffling of m*n size image. At the end, there were no changes in total size of image during encryption and decryption process. Encryption is very important to make sure that data that can be sent via communication channels are protected from being easily deciphering (Quist-Aphetsi Kester, 2013, [6]). The encryption processing technique is described as follows

Initially, the RGB colour was extracted from selected portion of the captured facial image. The ciphering of the selected portion of the image was done using by shuffling the RBG pixel values of the selected portion of the images. The RGB pixel values were transposed, reshaped and interchanged to obtain cipher image. There were no changes in bit value and no pixel expansion at the end of encryption process. This implies that the total change in all values of the image is zero. The RGB pixel is smallest element of an image which can be interchanged without negatively affecting the image size and quality.

B. Shanthi and Palanisamy (2014) A Novel Text to Image Encryption Technique by AES Rijndael Algorithm with color Code Conversation

This study proposed a scheme that focuses on block cipher substitution method to encrypt given text into blocks. Shanthi and Palanisamy extended that the main aim of cryptography is to enhance data confidentiality and privacy by making information unintelligent.

Methodology: It involves division of encrypted user given plain text into blocks .The encrypted text is in unreadable format. Each character of the block was shifted into ASCII value which is, in turn formulated into equivalent color code. For more enrichment to the encryption process, final encrypted text was obtained in image format. The following existing cryptography techniques were elaborated

(A) Symmetric Key Encryption
(B) Substitution Algorithm

Substitution Algorithm: Substitution Algorithm can be used as a type of operation that can transform plaintext to cipher text. Substitution of each element in Plaintext (Bit, Letter, Group of bits) can be mapped into another element(Shathi and Palanisamy, 2014, [10][11][12][13]) . The Plaintext can also be transposed after substitution to enhance mode of transforming data or image to unintelligible format.

C. Proposed Algorithm by Shathi and Palanisamy

Step 1: Read input text that is to be encrypted.
Step 2: Input text is encrypted through encryption algorithm and output is obtained.
Step 3: Encrypted unreadable format is divided in block ciphers of length 3 character per block.
Step 4: The block is replaced with three color codes, R, G, B respectively for each pixel within the block
Step 5: The entire known pixel contain three components like Red, Green and Blue. The magic of our algorithm three components range between 0 to 255 simultaneously ASCII table also contain 0 to 255.

Texts were represented and substituted into pixels in image format. The procedure for block substitution use RGB color image systems. A color is typically represented in three components intensities such as blue, green and red. Encrypted text were read and separated into three characters. The three characters were combined and consider as block. After the separation, into blocks, it was converted into corresponding color code to get a single pixel. The above process was repeated until full plaintext was converted into pixel. The pixel is used to draw 512× 512 image. The conversion of a sample message to ASCII values was demonstrated. The ASCII values that were obtained from sample message were divided and converted into block ciphers. Each block ciphers contain three characters per block. This is step by step process of sample text encryption into image and encrypted image can be later decrypted into text file. The use of secret key to restrict and monitor decryption process was not put into consideration.

© Copyright: All rights reserved.

D. Raju et al., (2012) A Secondary Fingerprint Enhancement and Minutiae Extraction

(Raju *et al.*, (2012), [9]) proposed fingerprint enhancement that involved Gaussian filter, binarization and thinning was introduced. It also consists of minutiae extraction and matching. To reduce hairy structures which lead to spurious ridge bifurcations and endings, a two dimension Gaussian filter was given as

$$F(x,y) = e^{-\frac{x^2+y^2}{2\sigma^2}}$$

Where σ is standard deviation. In this work, value of σ was 1.5.

Crossing Number (CN) was used to extract minutiae. The Crossing Number (CN) for a pixel P was given as

$$CN = \frac{1}{2}\sum_{i-1}^{8} |P_i - P_{i+1}|$$

Where P_i was neighborhood of P with binary value 0 or 1 and $P_9 = P_1$

(Philippe parra (2003), [5]) projected fingerprint Recognition that involves Binarization and Block filter. Minutiae were also extracted and matched. Binarization of gray scale image was done by fixing threshold value. Pixel value above and below threshold were set to '1' and '0' respectively. Block filter was used for thinning of binarized image by reducing thickness of ridges lines to single pixel width. To perform minutiae extraction and matching, Minutiae points were extracted by generating data matrix to get position, orientation and type of minutiae. Matching score of two images was computed, if matching score is 1, images were matched and if it is 0 then images mismatched.

III. ENCRYPTION AND DECRYPTION OF BIOMETRIC IMAGES

Cryptography is the process of hiding and protecting existence of message that can be inform of text, images and other form of information and data. Cryptography is normally done for the purpose of security and tamper prevention. Cryptography in this work involves encryption and decryption. The encryption is a process that involves conversion of biometric image encrypted images while decryption is reverse of encryption that is get back original image from encrypted images. During encryption process, biometric images (facial image and fingerprint were captured and stored in repository. Pixel values for each image can be obtained and used to generate pixel matrix of order I X J. The pixel values can be replaced by fixed numerical values by taking reverse order such that 0 can be encoded to 255, 1 as 254,……, 255 as 0. This is one of the way to re-shuffling pixel value to form encrypted image. Cipher matrix which is obtained can later be transposed. Password should be used to monitor and retreat access to the cipher matrix. Decryption is the reverse of encryption of every Cryptography Process. Cipher matrix can be decoded such that 255 will change to 0, 254 to 1 etc. Original Image will finally be obtained for decoded pixel matrix

A. Cryptography Process of the Model

Cryptography is described as science of encryption and decryption (Shanthi, Palamisam , 2014, [10]). Cryptography involves hiding the content of a message (video, image and other multimedia). There are different form of cryptography like binary cryptography and visual cryptography. There is need for protection of biometric images from intruders now that biometric system is generally accepted for accessing and identifying individual. (Quist-Aphetsi (2013), [6]) proposed a cryptographic image encryption technique. The encryption technique was based on RGB pixel shuffling of M × N size image. This cryptography was done to encrypt and protect selected facial area in connection to abuse cases on broadcasting media. The encryption involves reading of selected facial portion, extraction of red, green, and blue component. The red, green and blue component was later transposed, reshaped and concatenated. In this processes, the RGB values was shifted away from its respective positions and RGB values can be interchanged in order to obtain encrypted image. The encryption process proposed by Quist Alpetsi involves only component of the original image hence the encrypted image may be easily reverse to original image.

Also (Shanthi and Palanisamy (2014), [10]) proposed cryptographic algorithm that converted plain text into unintelligent form. The cryptographic algorithm focuses on block cipher substitution method that encrypted given texts into blocks which is similar to image format RGB. The algorithm demonstrated step by step process of text encryption to image format. This was achieved by converting ASCII value into block Cipher, three character per block. For instance, WELCOME with the following ASCII value 119, 101, 108, 99, 111, 109, 101 was converted to block cipher as follows. RGB (119, 101, 108), RGB (99, 111, 109) and RGB(101,0,0). All these encryption process utilized information and content of the original multimedia files that are constant. The cryptography process is divided into encryption and decryption module. Encrypting of Biometric images in this work entails hiding content of biometric images to prevent intruders or attackers from perceiving or having any knowledge about the images. The encrypting part of the model was achieved using Elliptic curve cryptography and Hill cipher Algorithm. According to (Dawahdeh *et al;* 2018, [4]) Biometric images was encrypted using an agreed elliptic function E. The encryption can be achieved by sharing domain parameters (a, b, p, G) where a, b are the co-efficient of the agreed elliptic function.

P is a large prime number

G is the generator point

Each user should choose randomly his private key from the interval [1, p-1]

- V_A for user A
- V_B for user B

Where V_A = private key for user A

V_B = private key for user B

The public key for each user will be generated by multiplying their private key with Generator Function G.

$P_A = V_A . G$ P_A = public key of user A

$P_B = V_B . G$ P_B = public key of user B

To get the initial key, each user multiples his private key by the public key of the other user to get the initial key

© Copyright: All rights reserved.

$S_i = (x, y)$
$S_i = V_A.P_B = V_B.P_A = V_A\ V_B.G = (x, y)$
$S_1 = x.G = [S_{11}, S_{12}]$
$S_2 = y.G = [S_{21}, K_{22}]$

According to (Acharya *et al;* 2007, [2]), 4 χ 4 self invertible key matrix (Km) will be generated from the initial key [S1 and S2]. This key will be used for the encryption and decryption process.

K_{11}	K_{12}	K_{13}	K_{14}
K_{21}	K_{22}	K_{23}	K_{24}
K_{31}	K_{32}	K_{33}	K_{34}
K_{41}	K_{42}	K_{43}	K_{44}

Km =

K_{11}	K_{12}
K_{21}	K_{22}

self invertible matrix, partition as Km =

K_{11}	K_{12}
K_{21}	K_{22}

It is assumes that K_{11} =

- The values of other partition of the secret matrix key Km was obtained by solving K_{12} = 256 - K_{11}, K_{21} = I + K_{11} and k_{22} = 256 - K_{21} , where I is the identity matrix
- The biometric image pixel values was later divided into blocks of four size that is a vector of size (4 by 1) (b_1, b_2, b_3,b_4). The encryption is done by multiplying the self invertible matrix (Km) by each vector modulo 256. The decryption is reverse of encrypting process that involves multiplying key matrix(km) by each encrypted vector and taking modulo 256. This is done to get the original image. If user A want to send encrypted image to user B, it must be done using an agreed elliptic curve function. For this experiment , the function is written below

$Y^2 = x^3 + 2x + 4 \bmod 31$

Where A= 2, B= 4, P =31 which satisfied the condition $4(A)^3 + 27(B)^2$

$= 4(2)^3 + 27(4)^2$
$= 32 + 432$
$= 464 \bmod 31 = 31$ not equal to 0
$Y^2 = x^3 + 2x + 4 \bmod 31$
$G(x,y) = (2, 4)$

The base point $E_{31}(2,4)$ can be chosen to represent enerator point G. If G(2,4) is the generator point, the parameters for E are { A, B, P,G} = {2,4,31,(2,4)}.

B. Key Generator

Each user choose his private key from the interval [1, p-1]

User A

- Choose the private key n_A = 4 E (1,30)
- Choose the public key $P_A = n_A.G = 4(2,4) = (2,27)$, 4(d) = 2(2d) d is a Point. 4(d) can be achieved using point doubling or point addition theory
- Compute the initial key $k1 = n_A.P_B = 4(30,27) = (28, 4)$
- Compute $k_1 = x.G = 28(2,4) = (25,16)$ and $k_2 = y.G = 4(2,4) = (2, 27)$ Key =

25	**16**
2	**27**

User B

- Choose the private key n_B = 2 E (1,30)
- Compute the public key $P_B = n_B.G = 2(2,4) = (30,27)$
- Compute the initial key $k_1 = n_B.P_A = 2(2,27) = (28, 4)$

25	16	232	240
2	27	254	230
26	16	231	240
2	28	254	229

Compute $k_1 = x.G = 28(2,4) = (25,16)$ K1 = And $k_2 = y.G = 4(2,4) = (2,27)$

The fingerprint image pixel values were separated into blocks of four size.

Table 1: Sample Fingerprint Pixel Value for Encryption of Image

116	103	67	47	37	35	28	42	47	59
102	64	41	49	17	65	18	72	35	69
118	60	47	84	15	108	16	98	33	66
128	72	54	118	20	144	22	116	41	56

Table 2: Encrypted Fingerprint Pixel Value through ECC

140	121	189	177	141	127	150	1120	183	75
128	70	105	193	129	177	170	116	153	119
158	90	229	66	151	110	150	120	217	232
122	226	198	22	232	252	14	102	251	162

C. Cryptographic and Steganographic Techniques of Information Security

Cryptography can be referred to as means for security confidentiality of information. Another form of information security is steganography to keep content and existence of a message or information secret. A typical example of steganography is a process of hiding passkey or message to image. The existence of the message is hidden in the image such that human eye cannot easily perceive the presence of the message in such image. Cryptography should not be misinterpreted for steganography. According to (Jassin (2013), [8][15]), the main difference between steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret. These two security techniques can be used and applied in secret agent for transmission of messages, graphics, image among others.

© Copyright: All rights reserved.

D. Fingerprint Minutiae Extraction

The fingerprint minutiae feature extraction was performed through a method called Crossing Number. The ridge ending points and bifurcation points also known as minutiae points can be determined by scanning local neighborhood of each pixel in fingerprint ridge image using a 3×3 window. Chouhan and Khanna (2011) revealed that feature extraction can be achieved through Crossing Number. Crossing Number is half sum of differences between pair of adjacent pixel. The ridge was denoted as ridge ending, when Crossing Number (CN) = 2 and if Crossing Number (CN) = 4, then ridge is bifurcation. This was achieved by scanning local neighborhood of each ridge pixel in fingerprint image using a 3 × 3 window. The crossing number was computed as half the sum of the difference between pairs of neighboring pixels N_i and N_{i+1}

$$CN_{x,y} = \frac{1}{2}\sum_{i=1}^{8}|N_i - N_{i+1}|$$

IV. IMPLEMENTATION OF THE MODEL

Before actually implementing a model into operation, a test run of the model should be done to remove bugs. It is an important phase of a successful model. After coding whole programmes of a model, a test plan can be developed and run on a given set of test data. This is done in Cryptographic Security for Fingerprint Verification System by selecting some sample of Biometric images that are not protected and encrypted. The encryption of fingerprint image is represented in Figure 1 while Figure 2 and Figure 3 shows encryption and decryption of ear and face image The cryptography process was implemented in a Graphical User Interface that entails Push Buttons (LOAD IMAGE, ENCRYPT IMAGE, and DECRYPT IMAGE) as indicated in the figure below. The load image buttons allow image to be selected and display as applicable during encrypting process. The selected image was later encrypted by clicking ENCRYPT IMAGE button. The encrypted image can be later decrypted through DECRYPT IMAGE button.

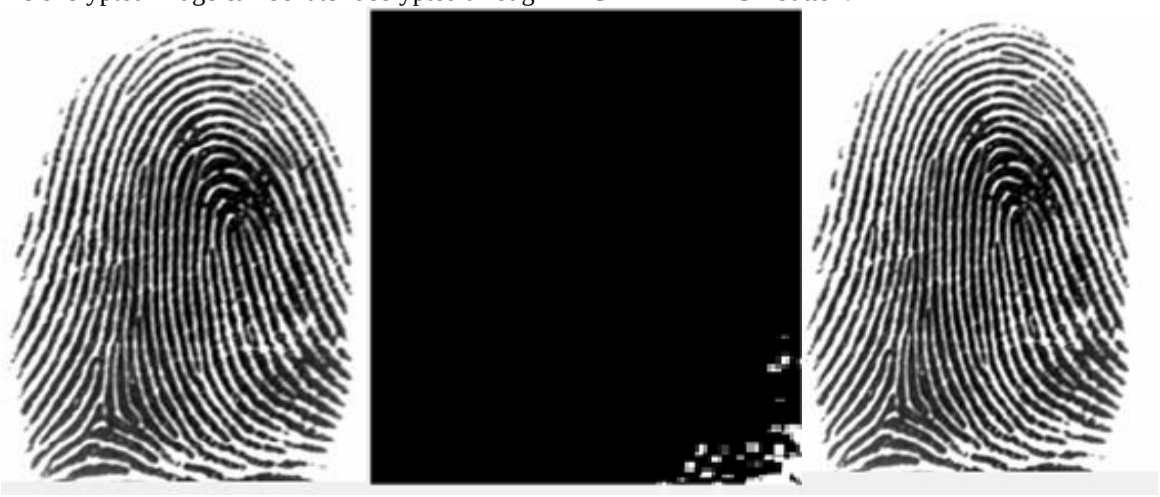

Figure 1: Cryptography Module of the Biometric Model

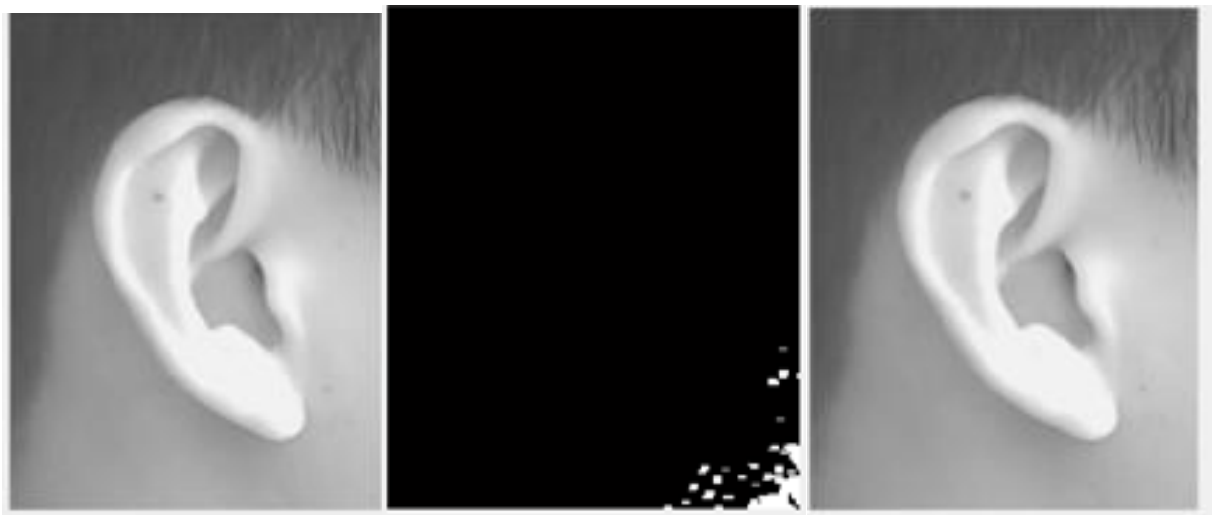

Figure 2: Encrypting and Decrypting of Ear Image

© Copyright: All rights reserved.

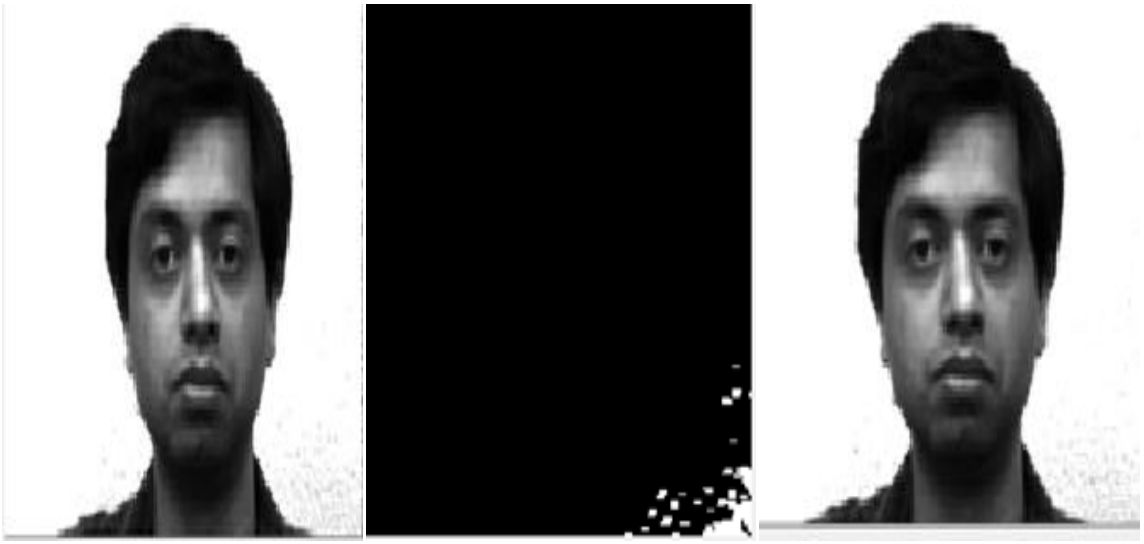

Figure 3: Encrypting and Decrypting of Face Image

Table 3: Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) of Encrypted Fingerprint Image

S/N	Fingerprint Image Filename.tiff	PSNR in Decibel(db)	MSE
1	101_1.tiff	24.1017	254.86.25
2	103_1.tiff	24.1473	252.2029
3	103_3.tiff	24.1571	251.6364
4	104_2.tiff	24.1090	254.4367
5	104_3.tiff	24.1090	254.4367
6	101_2.tiff	24.0994	255.0000
7	101_3.tiff	24.5417	230.3106
8	102_2.tiff	24.1090	254.4367
9	115_1.tiff	24.5417	230.3106
10	102_3.tiff	24.1319	253.0972

V. CONCLUSION

Cryptographic Security approach to Fingerprint Verification Model can be adopted to encrypt biometric images that are used in the following existing biometric system: Fingerprint Attendance System that can give account and correct details of worker's attendance in an organization, meetings, lectures, and conferences. Other Biometric System (BS) where Cryptographic Security method can be applied are Student Biometric ID card, Face Recognition System and Fingerprint Recognition System to prevent examination malpractices among others. It is very obvious that use of biometric trait is necessary to replace password that can be transferred and stolen. Hence, security aspect of existing biometric system is very important.

DECLARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of my knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Afsar F.A, Arif M. and Hussain M. (2004) Fingerprint Identification and Verification System using Matching, National Conference on Emerging Technologies PP 141-146
2. Acharya B., Rath G.S., Parra S.K. Panigraphy S.K. (2007) Novel Methods of Generating seif-invertible matrix for Hill Cipher Algorithm International Journal secur. 1(1)
3. Chaudhary V., Bhardwaj S., Sabharwa H. (2014) "Fingerprint Recognition using Orientation features" International Journal of Advanced Research in Computer Science and Software engineering. Research paper available online at www.ijarcsse.com. Vol 4, issue 5.
4. Dawahdeh Z. E., Yaakob S.N., R.R., Bin Othman (2018), " A new image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher" Journal of King Saud University-Computer and Information Science 30 (2018) 349-355. https://doi.org/10.1016/j.jksuci.2017.06.004
5. Philippe parra (2003) Fingerprint minutiae extraction and matching for identification procedure
6. Quist-Aphetsi Kester, (2013)" A Cryptographic Image Encryption Technique for Facial-Blurring of Images" International Journal of Advanced Technology and engineering Research (IJATER) www.ijater.com
7. Vivek K. S. , Tripatti S.P., Agarwal R.P. and Singl J.B. (2011) "Formal Verification of fingerprint ATM Transaction through Real Time Constraint Notation (RTCN) " (IJCSI) International Journal of Computer Science Issues, (8)(13)395:400. www.IJCSI.org.
8. Jassin F. A. (2013) . "A Novel Steganography Algorithm for Hiding text in Image using Five Modulus Method" International Journal of Computer Applications (0975-8887) Vol 72 No17.
9. Raju Rajkumar, Hemachandram (2012)" A secondary Fingerprint Enhancement and Minutiae Extraction, Signal and Image Processsing" An International Journal (SIPIJ) vol 3, No2 https://doi.org/10.5121/sipij.2012.3213
10. Shanthi, Palamisamy V. (2014) A Novel Text to Image Encryption Technique by AES Rijndael Algorithm with color code conversation, International Journal of Engineering trends and Technology (IJETT) Vol 13, No 15, PP 237-241 ISSN: 2231-5381. https://doi.org/10.14445/22315381/IJETT-V13P249
11. Yuliang .H, Jie T., X ipingL, Taughui Z. (2003) "Image enhancement and minutiae matching fingerprint verification" Pattern recognition letters Vol 24 pp 1349-1360 https://doi.org/10.1016/S0167-8655(02)00376-8
12. Saravanan, S., & Sivabalakrishnan, M. (2019). A Framework for Digital Image Encryption using Chaotic Baker Map with SHA Algorithm. In International Journal of Innovative Technology and Exploring Engineering (Vol. 2, Issue 9, pp. 4093–4097). https://doi.org/10.35940/ijitee.b7716.129219
13. Archana, N., Manogna, S., Hussain, Dr. M. A., & Razia, Dr. Sk. (2019). Secure Sharing of Documents using Image Encryption and Key Image. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 8, Issue 4, pp. 9415–9419). https://doi.org/10.35940/ijrte.d9724.118419

© Copyright: All rights reserved.

14. Janani, S., Shalini, M., Parkavi, K., & Chandrasekar, A. (2019). Autonomous Data hiding in an Encrypted Image using KM-DH Algorithm. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 2, pp. 4950–4952). Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP. https://doi.org/10.35940/ijitee.a4524.129219
15. Vejare, R., Vaish, A., Singh, K., & Desai, M. (2022). Removal of Image Steganography using Generative Adversarial Network. In Indian Journal of Artificial Intelligence and Neural Networking (Vol. 2, Issue 4, pp. 6–10). Lattice Science Publication (LSP). https://doi.org/10.54105/ijainn.d1054.062422
16. Proença, M. da C. (2022). On the Need of Quick Monitoring for Wildfire Response from City Halls. In Indian Journal of Image Processing and Recognition (Vol. 2, Issue 3, pp. 1–4). Lattice Science Publication (LSP). https://doi.org/10.54105/ijipr.c1014.042322

AUTHORS PROFILE

Akinribido C. T. is currently in the department of Computer Science. She is resourceful, effficient and effective. She is thorough, intelligent, trustworthy and hardworking. She has also attended several conferences. Her research interest is in Biometrics, Artificial Intelligent, Information Systems and Information Storage and Retrieval.

Olabode, O. is a lecturer in Computer Science Department. His research interests are Pattern Recognition and Security Data mining. He is thorough, intelligent, trustworthy and diligent He has to his credit, several articles published in International and National journals.

Adetunmbi A.O. is a Lecturer in Computer Science department. He is a member of Computer Profession of Nigeria (CPN) and MIEEE. His research interests are information security, Data Minimg and Computational Linguistic. He is thorough, intelligent, trustworthy and diligent. He has to his credit, several article published in International and National Journal.

Adewumi M.G. is a lecturer in computer science. Her area of interest are Computer Vision and Information Security. She is thorough, intelligent, trustworthy and dependable. She holds publications both local and international to her credit. She has passion for research. Olojo Oludare Jethro . is a lecturer in computer science. His area of interest are Computer Vision and Information Security. He is thorough, intelligent, trustworthy and hardworking. He has many scholarly articles to hiscredit. He teach courses in Computer Education. Olusola Theophilus Faboya is a lecturer in the Department of Computing and Information Science. His research interest include AL development, Modelling and Analytics of Human-centric Behaviour in socio-technical systems.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/ or the editor(s). The Lattice Science Publication (LSP)/ journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© Copyright: All rights reserved.