Survey on Encryption Approaches for Secure Face Biometrics

Kavya R
St.Josephs College Of Engineering And Technology, Palai
E-mail: kavyar132@gmail.com

Angitha George
St.Josephs College Of Engineering And Technology, Palai
E-mail: angitha.george@sjctgalai.ac.in

Abstract. Biometric system is twisting up logically basic since they give strong moreover, compelling techniques for character affirmations. The face recognition is the most trademark methods for biometric conspicuous verification and give versatile biometric affirmation and is a development prepared for serving an extensive variety of security application. This paper deals with the examination of different encryption approaches like AES, DES, and RSA that can be used for go up against face recognition security suggests and moreover analyze DNA cryptography. With the examination of these systems, AES gives sublime security while considering face affirmation.

Keywords: Biometric, Face Recognition, AES, DES, RSA, DNA cryptography.

1. Introduction
The multiplication of security issues identified with the validness of the people, there is a solid requirement for confirmation and validation frameworks. Today human confirmation can be classified as What you know, e.g secret key, individual check number; What you have, for example, a token, smart card and so forth and What you are, biometrics.

The initial two classifications are less secure techniques when contrasted with the biometrics. Brute compel assaults, Shoulder surfing, and phishing assaults are influenced by the passwords and individual check numbers. The initial two verification classes are shared among the collaborators and gatherings, which influence the security levels of the framework.

Biometric verification outperforms What you know and what you have. Biometric depends on the inherent parts of the human. Exact distinguishing proof, responsibility, simple and safe for utilize and remarkable individual ID are the principle advantages of biometric validation and assuming control conventional passwords and Id card confirmation. In light of the special highlights and about difficult to produce, individual to be distinguished to be physically present for the purpose of the confirmation. Physically, the individual to be distinguished at the present purpose of the check procedure. This trademark eases the confinement of utilizing a secret word or token that can’t separate between an honest to goodness client and a gatecrasher. Also, biometric highlights are an effective weapon against the dismissal of a proposition or thought.
Biometric security giving access to an individual in light of check of one's physical attributes. Biometric data is can’t transferable and share-able. The possibility of assault is less when contrasted with different frameworks.

These days the installment approaches by means of the web and the system have been developing at an enraged pace. Along these lines, the assortment of the electronic installment frameworks comprises of various kinds to accomplish a solid level of the security. Be that as it may, in parallel, the assaults techniques and methodologies are as cutting edge as the security arrangements. In this thorough overview, we attempted to specify distinctive encryption approaches for securing face biometrics. Encryption calculations utilized for securing information by encryption and unscrambling process.

2. Background
This area gives an outline of the diverse encryption calculations for the face acknowledgment biometric framework. An encryption calculation is a segment of information transport security and the way of changing over plain content to figure content, and after that back to the plain content for securing electronic information. We are adopting three encryption strategies those are DES, RSA, and AES.

- Data Encryption Standard (DES): DES (Data Encryption Standard) algorithm used as a standard practice for securing unclassified and sensitive data.
- Advanced Encryption Standard (AES): The benefits of AES is the high speed.
- Rivest-Shamir-Adleman (RSA): The Public key algorithm for encrypting the data.
- DNA Cryptography: New emerging domain form on DNA computing.

2.1. Face Recognition
Face Recognition is the most normal methods for biometric distinguishing proof and give adaptable biometric confirmation facial acknowledgment is an intense innovation fit for serving a wide range of security application. Facial acknowledgment can substitute the watchword for the gadget and the client account get.

Facial acknowledgment frameworks are computerized frameworks that confirm the people by contrasting the facial qualities, for example, remove between eyes, mouth, nose, and ear. These qualities are broke down and contrasted all together with distinguishing or confirm the people. Biometric face system follows the following stage of operations:

- Capture the biometric sample of the person.
- Extract set of relevant features from the captured sample.
- Compare the extracted feature set against the template set in the database.

Various calculations, these are identified with the face acknowledgment. Face acknowledgment calculation can be partitioned as two: geometric component based and appearance-based. Appearance-based techniques incorporate Eigenfaces [1], principal segment examination (PCA) and direct discriminant investigation (LDA), Independent Component Analysis (ICA), Kernel Principal Component Analysis (KPCA) [9], Kernel Fisher Discriminant Analysis (K FDA) [3], General Discriminant Analysis (GDA), and Support Vector Machine (SVM) [10]. The disadvantage of appearance-based techniques is that the face acknowledgment under a specific lighting can be performed dependably when the face has been already observed under comparable conditions. In appearance-based strategies, the caught highlights are the worldwide highlights, so these are hard to deal with.

The principal point of the geometric component based technique is to locate an arrangement of agent highlights from the image. Points, surfaces, and bends are joined together to shape the geometric features. These highlights of the pictures are seen by the element recognition strategies.
Geometric component based strategies are powerful in perspectives, however, include extraction process are touchy. The geometry highlight based techniques incorporate an itemized examination of the components or structure of nearby facial highlights. The geometry highlight based strategies incorporate Active Shape Mode and Local Feature Analysis (LFA). Acknowledgment of appearances from still pictures or 2D pictures is a troublesome issue, with the clarification, particular position and demeanor changes in the pictures make factual contrasts and face character winds up shadowed by these components.

2.2. DES (Data Encryption Standard)

In 1975 at IBM lab, Horst Feistel created DES. In 1978, the National Bureau of Standards, now called NIST has endorsed the DES. The DES was systematized by the American National Standard Institute(ANSI) as DEA (Data Encryption Algorithm).

\[\text{Figure 1. DES ENCRYPTION utilizing a picture.}\]

The most generally utilized symmetric square figure depends on the DES. For DES, information is scrambled in 64-bit pieces utilizing 56-bit keys and is a predecessor. Each square is scrambled in disengagement, which is a security helplessness. The key length of DES is expanded by the Triple DES. In triple DES, three DES task is performed on each square. By ordering encryption with key 0, a decoding with key 1 and an encryption with key 2. These keys might be interconnected.

DES displays exemplary Feistel structure, ensuing occasions, and open investigation appear in actuality configuration was suitable. DES has turned out to be broadly utilized, particularly in financial requests yet now it is supplanted by AES. For the DES encryption process, two contributions to the encryption work: the plain which is of 64-bits long and key size is 56-bits long. The little changes in the plaintext or key roll out critical improvements in the ciphertext. The change in plaintext or one piece of key deliver changes in numerous bits of the ciphertext(Avalanche impact). DES uncover solid torrential slide impacts.

2.3. Advanced Encryption Standard (AES)

\[\text{Figure 2. AES Design.}\]

AES is piece figure proposed to trade DES for business applications. It utilizes 128 piece square size and a key size of 128,129 or 256 bits. AES is to a great degree effective in a 128-bit
frame; AES utilize keys of 192 and 256 piece for encryption reason. AES considered impermeable to all assaults, except for beast compel, which endeavor to decode utilizing all conceivable blend in 128, 192, or 256-bit figure. AES is a symmetric figure actualized in both equipment and programming to secure computerized information.

AES does not utilize Feistel structure, rather each full round comprise of four separate functions: byte substitution, permutation, arithmetic activities and XOR with a key. In AES, all tasks are performed on 8-bit bytes. Ciphertext takes a plaintext piece size of 128 bits or 16 bytes. The key length can be 1624 or 32bytes(128, 192, 256 bits) and the calculation alludes as AES-128, AES-192, and AES-256 relying upon the key length.

2.4. RSA
In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman composed the RSA. Key generation, encryption, and decoding are the real strides for the RSA. RSA conspire is a square figure, the plaintext and ciphertext are the whole numbers in the vicinity of 0 and n-1 for some n and run of the mill estimate for n are 1024-bits or 309 decimal digits.

In advanced mark and encryption plans, RSA most generally utilized. Its security depends on the diculty of figuring substantial numbers. An advanced mark plot in light of RSA keeps running as takes after: assume p and q are two huge primes.

Compute $n = p \times q$
and choose $e$ and $d$ such that
$e \times d \mod (p - 1)(q - 1) \equiv 1$.
Each user has a key pair, which includes a private key and a public key. Suppose $d$ denotes the users private key, and $(e, n)$ denotes the users public key. When Alice wants to sign a message $M$ and sends it and its digital signature to Bob, Bob can verify whether the signed message was really signed by Alice as follows:

Sign:
- Alice computes $s = M^d \mod n$, where $d$ is Alices private key.
- The value $s$ is Alices signature on $M$. Then Alice sends Bob $(M, s)$.

Verify:
When Bob receives these messages from Alice, he can verify whether $s$ is Alices signature on $M$ by checking $s^e = M \mod n$, where $e$ is Alices public key.

2.5. DNA Cryptography
In 2005, Kazuo Tanaka proposed the DNA cryptographic approach in light of open key. DNA Cryptography can be characterized as a concealing information regarding DNA Sequence. Cryptographic strategy in which each letter of the letters in order is changed over into an alternate blend of the four bases that make up the human deoxyribonucleic corrosive (DNA). It comprises of regular cryptographic methodologies key age, encryption and unscrambling process.

The DNA strand made up of agglomeration of nucleotides, which comprise of four nitrogen bases: Adenine, Cytosine, Thymine, Guanine. The letter A, C, T, and G are nucleotide bases. Adenine (A) make combine with Thymine (T) and Cytosine(C) with Guanine(G). These bases make the match with each other to frame base sets, to make twofold helix structure of DNA. DNA cryptography gives Unbreakable security.

DNA cryptography for the biometric confront framework come behind the resulting stages:
- Image is used under the form of ASCII code.
- Numbers are grouped into blocks and encrypted.
- Encoded message is changed into binary format.
• Digits are grouped into two and substituted as A- 00, T-01, G-10, C-11.
• Fit primers on either the side of the code.

3. Comparative Study on algorithms

| Parameters          | DES          | AES          | RSA          |
|---------------------|--------------|--------------|--------------|
| Developed           | 1977         | 2000         | 1978         |
| Keysize             | 56 bit       | 128,192,256 bits | 1023 bits    |
| Blocksize           | 64 bits      | 128 bits     | Mim 512 bits |
| Cipher/ Decipher key| Same         | Same         | Different    |
| Algorithm           | Symmetric    | Symmetric    | Asymmetric   |
| Encryption          | Moderate     | Faster       | Slower       |
| Decryption          | Moderate     | Faster       | Slower       |
| Security            | Slightly Secure | Excellent   | Insecure     |

4. Conclusion

The understood overview for the most part centered with considering around various encryption approaches utilized for confront acknowledgment. Encryption calculation assumes an imperative part of security. In this review, we break down various encryption approaches like AES, DES and RSA calculations and discovered AES indicates critical security while thinking about DES and RSA. DNA cryptography is a rising innovation give unbreakable security. The near table demonstrates the confirmation of the investigation.

References

[1] Michael Goh and David Ngo, "PalmHashing: a novel approach for dual-factor authentication", Pattern Analysis and Applications, Vol. 7, Issue 3, pp 255268, 2004.
[2] Abate, F, Nappi M, Riccio D, and Sabatino G, Face recognition: A survey, Pattern Recognition Letters, Vol. 28, pp. 1885-1906, 2010.
[3] M. Kumar and E. G. Dharma, A comparative analysis of symmetric key encryption algorithm, IJARCET, vol. 3, no. 2, 2014.
[4] Achermann B., Jiang X., and Bunke H, Face recognition using range images, In International Conference on Virtual Systems and MultiMedia, pp. 129136, 1997.
[5] Nyo Htweand Nu War, "Human Identification Based Biometric Gait", International Journal of Advanced Research in Computer Engineering Technology, Vol. 2, no 5, 2013.
[6] E. Biham and A. Shamir, "A differential cryptoanalysis of data encryption standard", Springer-Verlag, 1993.
[7] S. Basin, International data encryption algorithm (idea) a typical illustration, Journal of global research in computer science (JGRCS), Vol. 2, no 7, 2011.
[8] A. Kakkar and M. L Singh, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multimode Network, Published in International Journal of Engg and Technology(IJET), Vol. 2, no. 1, 2012.
[9] Andrew Teoh, BengJina David Ngo, and ChekLinga Alwyn Gohb, "Biohashing: two-factor authentication featuring fingerprint data and tokenized random number", Pattern Recognition, Vol. 37, no 11, 2004.
[10] L. Singh and R. K. Bharti, "Comparative performance analysis of cryptographic algorithms", International Journal of advanced research in computer science and software engineering (IJARCSSE), Vol. 3, no. 11, 2013.
[11] W. Zhao, R. Chellappa, P. J. Phillips and A. Rosenfeld, Face Recognition: A Literature Survey, ACM Computing Surveys, Vol. 35, no. 4, pp. 399458, 2003.
[12] Joseph P. Campbell, Face Recognition: A Tutorial, Proceedings of the IEEE, Vol. 85, no. 9, September 1997.
[13] Anna Labb and Annie Prez, "AES Implementation on FPGA: Time - Flexibility Tradeoff", 12th International Conference on Field-Programmable Logic and Applications, pp 836-844, 2002.
[14] D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal Research Develop., vol. 38, no. 3, pp. 243-250, 1994.
[15] R. Davis, The data encryption standard in perspective, Communications Society Magazine, IEEE), pp. 59, 2003.
[16] A.Sindhuja, B.Sri Nandhini, S.Bharathi, and I.Kalaimathy, "A Hybrid Authentication System Using Biometrics and Text Compression", International Journal of Scientific and Research Publications, Vol. 3, no. 3, 2013.
[17] Dr. Prerna Mahajan and Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web Security, Vol. 1, no. 15, 2013.