# A Unique hybrid cipher mechanism for effective, secure & reliable communication

Pankaj Rakheja, Saransh Gupta, Ruchika Sachdeva, Radhika kandhari

**Abstract**— Information flowing through the network need to be secured and communication needs to be made reliable as most of the transactions carried out are highly confidential .Integrity of information needs to be maintained. Traditional cryptographic mechanisms are now not that reliable. New cryptographic schemes like DNA cryptography, elliptical cryptography, quantum cryptography, biometric cryptography etc are emerging in today's scenario. Biometric cryptography ensures authentication to highest degree. Biometric cryptography technique uses biometric features to encrypt the data, which improves the security of the encrypted data and overcome the shortcomings of the traditional cryptography. This paper proposes a novel biometric cryptographic algorithm based on the most accurate biometric features like iris and fingerprint. It inculcates the benefits of traditional cryptography, biometric authentication and steganography in a single cipher mechanism to make it immune to new advanced attacks on data flowing through media over the globe.

**Index Terms**— authentication, cipher, Digital watermarking, LSB insertion, ridges, steganography, valleys,

## 1 INTRODUCTION

Information maybe local or of global scope flows throughout the network.. It is required to secure that information to prevent unauthorized access of it by any possible means. We must ensure a secure infrastructure that opens up just enough doors that are mandatory to protect everything else. We need to ensure privacy, integrity and confidentiality in the network so that it is reliable and dependable for information exchange and for that we encode the data before sending it using different encoding mechanisms to make it non readable thus meaningless. This is where cryptography[1-5] is needed.It is the art and science of achieving security by encoding the simple message to make it unreadable.There are basically two types of cryptographic techniques for converting plaintext to cipher text and vice versa - symmetric and asymmetric cryptography. In symmetric cryptography sender and receiver use the same key for encryption and decryption of text shared by a reliable third party after authentication phase whereas in asymmetric cryptographic systems two different keys namely public and private keys are used for encryption and decryption process here data is encrypted using public key and decrypted using private key.

Here, we will be working on advanced data encryption algorithm which comes under Symmetric cryptography. AES is based on the block cipher Rijndael and became the designated successor of the Data Encryption Standard (DES) which has been implemented in a tremendous number of cryptographic modules worldwide since 1977. It came in 2001. Since then it has proven to be an efficient encryption mechanism as it is immune to most of the differential and linear attacks. It is based on a design principle known as a Substitution permutation network. This makes it fast in both software and hardware in processing and implementing. AES is a block cipher with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size do has a maximum of 256 bits, but the key size has no theoretical limit. It operates on a 4×4 array of bytes, termed the *state* Most of the AES calculations are done in a special finite field. Finite field arithmetic limits the results size to finite length to carry out further operations of substitution, permutations etc.

The basic structure of AES relies on redundant modular operations carried out for certain rounds. that includes round constant generation , substitution boxes , shifting of rows , key expansion etc which are well known to attackers also and they are developing new sort of attacks to break it down for decades and with advancement in the fabrication technology and networking architectures better resources are available now and many new types of attacks like Courtois and Pieprzyk attack, conceivable timing attacks on AES have been developed and in order to make it secure and immune against these attacks or the ones to come ahead we are applying biometric features for carrying out authentication so that only the desired receiver only should be able to get the message for that we are taking fingerprints which are a unique identification mark for an individual. Morover as we know that if we can hide the existence of any message encrypted or not itself makes it secure to being attacked so we are also inculcating a module which actually hides the cipher text and a share generated from the fingerprint of a register candidate for which message is destined in a cover image which actually is transmitted along the media using LSB insertion mechanism[6].

This paper basically describes our designed mechanism in a systemmetic manner section I describes basic cryptography and AES and brief of designed mechanism, section II describes AES, Biometric features and LSB insertion method which hides information in an image, section III describes our designed mechanism in detail, section IV comprises of results obtained after simulation, section V concludes the paper and atlast we have mentioned various valuable references that comes under literature survey carried out by us.

## 2 OVERVIEW

### Advanced Encryption Standard

The AES algorithm [3] [5] is a subset of the Rijndael algorithm it is basically a lock cipher. it uses a 128 bit block and three different key sizes 128, 196 and 256 bits, where Rijndael allows multiple block sizes 128, 196, and 256 bits and for each it also allows multiple key sizes, again 128, 196, and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used to both encryption and decryption of a message. Also, the cipher text produced by the AES algorithm is of the same size as that of plain text message

Most of the operations in the AES algorithm take place on bytes of data or on words of data 4 bytes long, which are represented in the field GF ($2^8$), called the Galois Field.

The input (block size $N_b$, also known as plaintext) of the AES algorithm is converted into a 4 x 4 array, called a state. Four methods, Addround key, substitution from S box, Shifting rows and mix column operations perform various operations on the state to calculate the output state (the final cipher text).

AES is designed for effective implementation using bytes. The AES algorithm loops through certain sections $N_r$ times. The AddRoundKey is performed at the beginning and at the end of the cipher in order to provide initial and final randomness to the algorithm. Without this, the first or last portion of the cipher could be easily deduced, and therefore would be irrelevant to the security of the cipher. The last round in the cipher is different from the other rounds in order to make the encryption and decryption routines more similar, allowing the complexity to be reduced in hardware, and software, implementations. The flow chart of encryption and decryption process is shown below in figure 1 and figure 2.

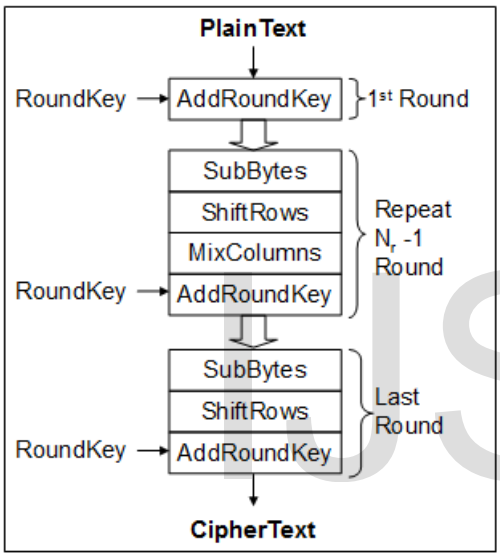



Figure 1: Encryption process

**AddRoundkey**

Here sate matrix is Xored with key matrix

**SubBytes**

Here we use substitution box where element of state matrix are substituted from an element of Substitution box

**Mixcolumns**

Here modulo arithemetic multiplication and addition of state with key and poly matrix occurs

This whole processes is reversible with correct key we can decode the ciphertext to get back the plaintext

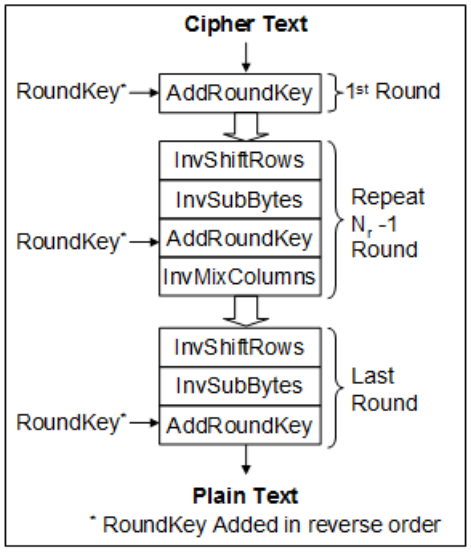



Figure 2: Decryption process

**AddRoundkey**

Here sate matrix is Xored with key matrix

**InvSubBytes**

Here we use inverse substitution box where element of state matrix are substituted from an element of inverse Substitution box

**InvMixcolumns**

Here modulo arithemetic multiplication and addition of state with key and poly matrix occurs to get the plaintext from ciphertext. It is inverse of Mixcolumns

## BIOMETRICS

Biometrics[9-10] basically deals with verifying the identity of a person based on the physiological or behavioral characteristics. Various technologies under it may be

.

**Fingerprint Recognition**

The fingerprint is composed of various 'ridges' and 'valleys', which form the basis for the loops, arches and swirls on your fingertip. The ridges and valleys contain different kinds of breaks and discontinuities known as 'minutiae'.Fingerprint images are scanned and converted into templates. Fingerprint recognition is most commonly used biometric technology as it is easily available and reliability is high.

**Facial recognition**

It includes extraction of facial features like distances from or between the ears, nose, eyes, mouth and cheeks.

**Iris and retinal recognition**

Unique features of the iris are examined. The iris is the colored section between the pupil and the white region of the eye, used to control the size of the pupil (allows light to pass through). The unique features of the iris include the meshwork (the tissue that gives the iris its 'radial' impression). In this the boundaries of the iris are defined and coordinate grid over the image is created. All the selected characteristics within the zones are then stored in as individual's biometric template.

Retinal recognition: examination of the pattern of blood vessels in the retina, which is located at the back of the eye. Is done, it focuses on the area where the nerve leaves the brain and enters the eye.

**STEGANOGRAPHY**

**Share generation** [6-8] deals with generating 'n' shares of the black and white image to be encrypted. Here we have used the simplest access structure which is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption. These shares are random dots without revealing the secret information.
The back pixel is denoted by 1 and white pixel as 0.

**Element division** is the technique in which every image is divided into two arrays one with the elements at odd positions and the other with elements at even position.

**Digital Watermarking**- have been proposed recently as the means for ownership protection of multimedia data. Represents a watermarking-based visual cryptography scheme with meaningful shares is to embed a hidden watermark message into a host object such that the hidden message is inseparable. Earlier watermarking was applied to text only. Now days watermarking is applied to all types of media. The scheme does not change the original pixel expansion, and not only applies for black and white binary images, but also for any gray and color images. Meanwhile, the embedded image in a meaningful share is robust. Before and after being extracted the image's quality did not change significantly. The scheme is easy to implement and highly feasible. There are many research articles exploring the watermark method Digital watermarking is applied to video also to stop piracy which results in loss of revenue. There should be no perceptible difference between the watermarked and original signal, and the watermark should be difficult to remove or alter without damaging the host object.
Here in the host object we insert the the secret message in form of image or text at the LSB position of the host object which can later be extracted back.

## 3 MECHANISM DESIGNED

We have designed a Biometric cryptographic mechanism which will use AES cipher in itself just as an additional round which data has to go through for encryption. It provides better efficiency and effectiveness then both individually.
For encoding of data we are using the AES algorithm whose encrypted text is hidden in a cover image. This even hides the existence of secret message flowing through the media and makes it less vulnerable to attacks. Then as we are hiding an encrypted text in the image so even after getting the text hacker won't be able to crack it as he does not have the key. Secondly we have used biometric authentication for enabling only the desired recipent to open the message but for enabling that we need to include sensors in mouse or laptop touchpad so that the user does not even know that his finger prints are being taken. This mechanism is designed for military and commercial purpose as there most of the information is confidential and unauthorized access is threat to the overall system. And as we know most of the MNCs and even in defense biometric initials like fingerprints are taken so we can use them as a database.

Encryption steps are explained through a flowchart in figure firstly we acquire fingerprint of the recipient from the database generate shares by taking even and odd position bits and then hiding one of the shares in the cover image and then take the plaintext to be encrypted and apply AES algorithm on it and insert the cipher text using LSB encryption technique

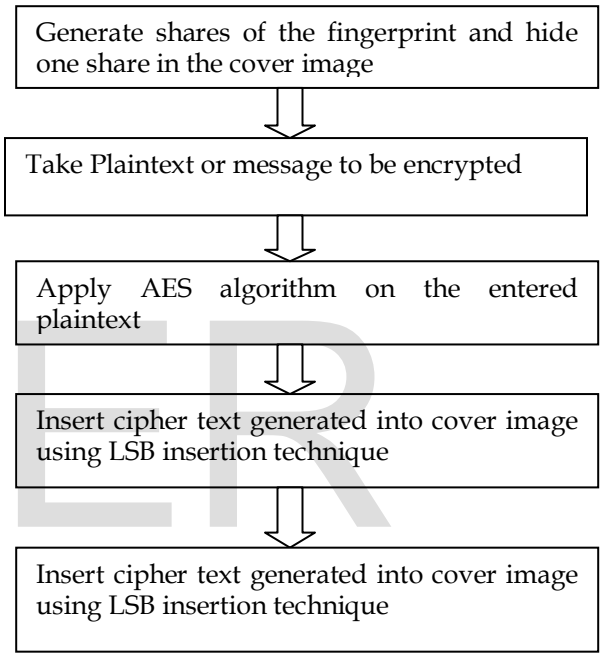
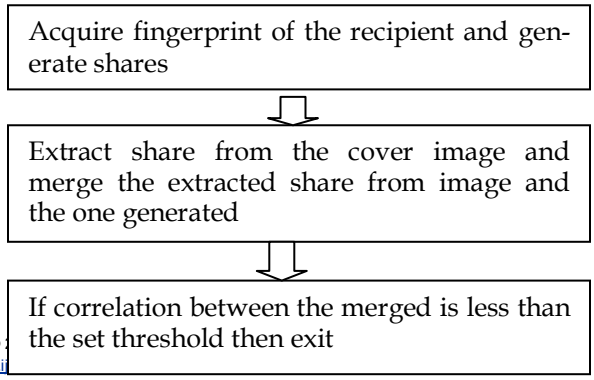



Figure 3: Encryption process

While at the receiver side the steps to be followed are shown in flowchart in figure. Firstly on acquiring the image which contains secret information we acquire recipient's fingerprints first then generate shares and on merging the share extracted from the image and the one from recipient we compute correlation between two and if it is above set threshold of 98.5 percent then algorithm extracts the cipher text and decodes it using AES decryption process else it displays that cover image only



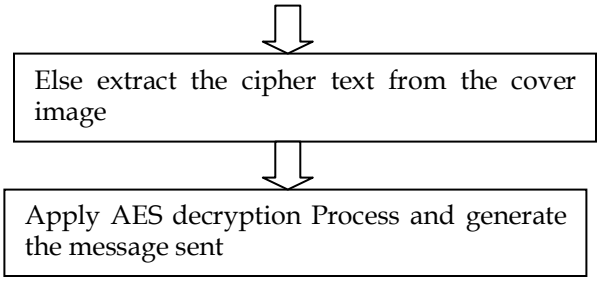



Figure 4: Decryption algorithm

Share generation process [6-8] works as shown in figure here on acquiring the fingerprint its binary image is generated and the two shares one with odd and the other with even position bits. One of which is inserted in the cover image.

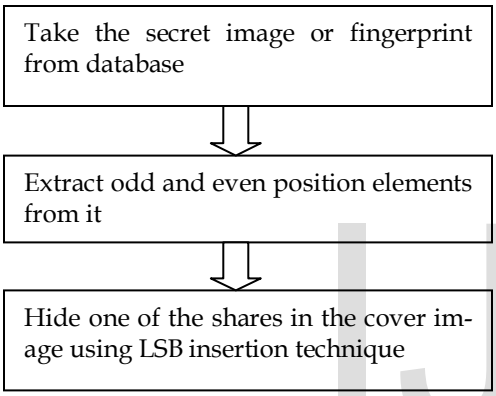



Figure 5: Decryption algorithm

## 4 RESULTS

For carrying out implementation of the cryptographic mechanism designed we have used Matlab, which is a matrix-oriented programming language, perfectly suited for the matrix-based data structure of AES, image based steganography and biometric share generation and operations as they all relly on Matrix based computations. The plaintext after undergoing encryption and decryption process employed here has successfully been recovered for the if the the correlation is above set threshold and most important the PSNR of cover and watermarked images is infinity which shows that even after inserting cipher and fingerprint share they both are identical. Figure shows cover image, grayscale image used for inserting, fingerprints, shares generated and we have shown the results in a proper sequence first text gets encrypted then if fingerprints match then only encrypted text gets extracted else the same image is shown and cipher text is made zero too.

```
*******************************************
*                                         *
*          C I P H E R                    *
*                                         *
*******************************************
```

```
Initial state :     00 44 88 cc
                    11 55 99 dd
                    22 66 aa ee
                    33 77 bb ff
Final state :       69 6a d8 70
                    c4 7b cd b4
                    e0 04 b7 c5
                    d8 30 80 5a

hidden text =

696ad870
c47bcdb4
e004b7c5
d830805a

f =

01101001
01101010
11011000
01110000
11000100
01111011
11001101
10110100
11100000
00000100
10110111
11000101
11011000
00110000
10000000
01011010

PSNR = +  Inf dB

*******************************************
              WELCOME
          ACCESS GRANTED
*******************************************
Encrypted text is
69
6A
D8
70
C4
7B
CD
B4
E0
04
B7
C5
D8
30
80
5A
```

```
*****************************************
*                                       *
*    INVERSE CIPHER                     *
*                                       *
*****************************************

Initial state :     69 6a d8 70
                    c4 7b cd b4
                    e0 04 b7 c5
                    d8 30 80 5a
Final state :       00 44 88 cc
                    11 55 99 dd
                    22 66 aa ee
                    33 77 bb ff
```

**STEGANOGRAPHY PART**

Cover image grayscale image

Fingerprint of desired and unauthorized recipent

Shares generated of desired recipent

Shares generated of the unauthorized recipient

Figure 6: Steganography results

## 4 CONCLUSION

Biometric cryptography ensures authentication to highest degree. Biometric cryptography technique uses biometric features to encrypt the data, which improves the security of the encrypted data and overcome the shortcomings of the traditional cryptography. Here the steganography implementation even hides the existence of any secret message thus makes it less vulnerable to attacks and simulation shows that if an authorized user tries to access the information stored in the image he is not able to get it as his fingerprints won't match and then cipher extraction won't occur and he won't be able to access ciphertext itself, decoding that is not even possible then.

Thus biometric authentication along with steganographic technique implementation in advanced encryption standard makes it more efficient and secure. Future implementation may include hiding multiple shares that is K out of N shares to make it more difficult to extract shares.

## REFERENCES

[1] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and SourceCode in C", John Wiley & Sons, Inc, 1996.

[2] Piper," Basic principles of cryptography" , IEEE Colloquium on Public Uses of Cryptography, 1996

[3] Sanchez-Avila, C. Sanchez-Reillol, "The Rijndael block cipher (AES proposal) : a comparison with DES" 2001 IEEE 35th International Carnahan Conference on Security Technology

[4] Sakalli, M.T. Bulus, E. Buyuksaracoglu, F," Cryptography education for students", ITHET 2004 Proceedings of the Fifth International Conference on information Technology Based Higher Education and Training, 2004.

[5] Atul Kahate ,"Cryptography and Network Security", Tata Macgraw Hill,2009

[6] Juneja, M.; Sandhu, P.S.;"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption" ARTCom '09. International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[7] Ching-Sheng Hsu and Shu-Fen Tu," Digital Watermarking Scheme with Visual Cryptography" Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong

[8] Gokul.M, Umeshbabu R, Umeshbabu R, Deepak Karthik, " Hybrid Steganography using Visual Cryptography and LSB Encryption Method" International Journal of Computer Applications (0975 – 8887) Volume 59– No.14, December 2012

[9] Mrunal Fatangare, K.N.Honwadkar," A Biometric Solution to Cryptographic Key Management Problem using Iris based Fuzzy Vault" International Journal of Computer Applications Volume 15– No.5, February 2011

[10] Biruntha.S, Dhanalakshmi.S, Karthik.S, PhD," Survey on Security Schemes for Biometric Privacy" International Journal of Computer Applications Volume 60– No.1, December 2012