RGB Based Visual Steganographic Cipher Mechanism Integrating Biometric Authentication in RSA

Pankaj Rakheja, Ritu Malik, Shivali Gupta

Abstract— Cryptography is the art of making human readable text to non readable for ensuring secure communication over the network. There are broadly two types of cryptographic schemes one is symmetric cryptography and the other is asymmetric cryptography. In the symmetric cryptography we use single key for encryption and decryption which creates problem of key sharing whereas in asymmetric cryptography different keys are used for encryption and decryption so key sharing is not a problem. But now traditional cryptographic ciphers are prone to different attacks and problem of authentication also exists. So we have integrated biometric and visual cryptographic modules in the basic RSA module to make it more secure. The RSA encrypted text or message is hidden through LSB insertion in RGB components of an image which also has shares of the fingerprint of the desired recipient. The receiver would be able to get the message only if his fingerprints matches to that of the desired one else he would just be able to see image only that is we have hidden the existence of secret message so as to make it even more secure. Computer simulation has been carried out to validate the proposed technique

Index Terms— AES, Biometric,cipher, DNA, LSB, RSA, Steganography

1 INTRODUCTION

These days, a lot of data is continuously being transferred over the internet. Most of this data is random but some of it is of high importance and needs to be protected from access by other users. For this we use the technique called cryptography, which is the science of making data non-readable by encoding it. This can later be converted back to readable format after being safely transferred over the internet to the rightful owner, sometimes even without knowing how it was initially converted. This process is called decryption of data.

Cryptography [2] [6][7] is the practice of secure communication of data in the presence of third party. Cryptography dates back to 1900 BC when an Egyptian scribe used non standard hieroglyph in an inscription. It includes overcoming the various antagonists which are related to aspects of information security like data confidentiality, data integrity, data authentication, data validity, privacy, non-repudiation etc. It includes encryption, i.e. converting secret data into apparent nonsense so that only intended recipients can recover original information. Decryption is the exact opposite of encryption. This usually involves the same keys and algorithms as used for encryption. One can also use crypto analysis, i.e. Decoding messages without knowledge of the exact encryption techniques. Various types of cryptography techniques are available:

Symmetric (or secret or private) cryptography is the most widely used technique which involves a secret key being shared by both the sender and the receiver. The same key is used to hide the message by the sender and in opposite way, by the receiver, to reveal the message. Examples include twofish, serpent, AES, blowfish, etc.

Asymmetric (or public) cryptography uses a pair of keys, a public key and a private key. The public key is freely distributed, which is used by the sender to hide the message. Now, the message cannot be even revealed by the sender. The private key is kept secret by its owner and is used to reveal the message. Examples include Quantum cryptography, elliptical

cryptography, etc. DNA cryptography can be used with both public and private cryptography.

Computers perform fast calculations and can produce strong encryption algorithms. Examples are algorithms like RSA, AES, blowfish, etc.

People are better at patterns, variations in meanings, changing orders, but are slower than computers and these cryptography techniques can be broken easily. Examples include Caesar ciphers, straddling checkerboard, etc.

Visual cryptography [4][5] [8-10**]** is the cryptography technique which involves encryption of visual information like pictures, text, etc. so that decryption doesn't require a computer. It involves creation of multiple shares of the secret data which individually reveal no information about the data. They are useful only when all shares are combined which would decrypt the data. Moni Naor and Adi Shamir developed one of the best known visual cryptography techniques in 1994, which involved breaking an image into "n" shares, where any "n-1" shares revealed no information. Decryption was performed by overlaying all "n" shares together, to reveal the original image. Each share can be printed on a separate transparency, and can be used for one-time pad encryption, where one transparency acts as cipher text and another is a shared random pad.

2 OVERVIEW

All the methods used by us have been discussed below:

Share generation involves generating "n" shares of the available coloured image. All of these shares are required for successful decryption of the secret image.

Element division [3] 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.

Manchester encoding is a line code in which encoding of each data bit has at least one transition and takes the same amount of time which makes it self-clocking, therefore a clock signal can also be recovered from the encoded data. Its DC component carries no information allowing the signal to be conveniently conveyed by media which usually don't convey a DC component. This makes use of almost double the bandwidth than the original signal but has high tolerance to frequency errors and jitter in transmitter and receiver reference clocks.

Summary of Manchester encoding:

- Each bit is transmitted in a fixed time period.
- A low-to-high transition signifies a "1" and a high-to-low transition signifies a "0", according to IEEE 802.3 convention. (According to the G.E. Thomas convention, the reverse holds true)
- The transition at the midpoint of a period signifies the 0 or 1.
- The transition at the start of a period doesn't signify data. They exist only to place the signal in the correct state to allow the mid-bit transition.

Inversion of Manchester signal during communication may end up in its transformation from one convention to another, but this uncertainty can be overcome by using differential Manchester encoding.

Biometric encryption [11-13] is the method of using a body characteristic such as fingerprints, retinas, irises, palm print, facial structure, voice recognition etc. to encrypt or decrypt data. The uniqueness of these characteristics ensures security in communication over the internet. The non-biometric encryption processes, such as passwords are prone to attack by unauthorised users due to limited number or permutations possible depending upon the length of the password. They might also be lost, stolen or forgotten. Whereas biometric encryption has a personal identifier for this there is one unique perfect match.

- **Fingerprint matching** requires comparison of patterns of ridges, and minutia points, which are unique features. Arch, loop and whorl are the three basic patterns of fingerprint ridges. Ridge ending, bifurcation and short ridge are major minutia features

of fingerprint ridges. Fingerprint sensors capture a live scan image which is digitally processed to create a biometric template which is later used for matching. It is the most commonly used biometric technology.

- **Retinal scan** is a biometric identification technique which uses the unique patterns on a person's retina to identify them. It involves examining the pattern of blood vessels at the back of the eye. The blood vessels within the retina absorb light more readily than the surrounding tissue, making it easily identifiable using proper lighting.

- **Iris recognition** uses mathematical pattern-recognition techniques on video image of the iris whose pattern is unique. The algorithm detects and excludes outer parts like eyelid, eyelashes and analysis the set of pixels containing only the iris to extract a bit pattern encoding the information needed to compare two iris images.

- **Palm identification,** just like fingerprint identification, is based on information presented in a friction ridge impression. A palm print consists of principle lines, wrinkles and epidermal ridges. It also contains information such as texture, indents and marks which can be used to compare a palm to another.

- **Face recognition** involves the identification of basic geometrical characteristics of the face. Firstly colour segmentation is done to determine the proportion of skin tone pixels. Then high level features like eyes, nose, mouth are recognised, followed by recognition of low level features like parts of eyes, nose, eyebrows, etc. relative to high level features. A database is formed from statistics of approximate locations of these features. Recognition can now be carried out frame by frame using the training set constructed from the statistics.

- **Voice recognition** can be used to authenticate or verify the identity of a speaker. It can also be used to identify what is being said. This is based on difference in acoustic patterns like size and shape of throat and mouth, and behavioural patterns like voice pitch, speaking style. In *speaker verification* one speaker's voice is matched to one template, whereas in *speaker identification* the voice is compared against "n" templates.

RSA algorithm is the most popular asymmetric key cryptographic algorithm. It is based on the fact that it is easy to find large prime numbers and multiply them together, but it is extremely difficult to find the factors of their product. In such cryptosystem, encryption key is public and different from the decryption key, which is kept a secret. Process of encryption and decryption is as follows:

- Choose two large primary numbers P and Q.
- Calculate N = P*Q.
- Select the public key (encryption key) E such that it is not a factor of (P-1) and (Q-1).
- Select the private key (decryption key) D such that (D*E) mod(P-1)*(Q-1)=1
- For encryption, calculate the cipher text as CT from the plain text PT as $CT=PT^E$ mod N
- Send CT as the cipher text to the receiver.
- For decryption, calculate the PT from CT as $PT=CT^D$ mod N

This algorithm may fall prey to "man-in-the-middle" attack. To eliminate this problem we use steganography.

Steganography is the art of encoding hidden message which uses the concept of hiding the existence of the message. It comes from the combination of the Greek words "steganos" meaning "protected" and "graphei" meaning "writing". It has taken many forms since its origin in ancient Greece centuries ago and has vast applications even in the modern society. In 1518 Johannes Trithemius wrote the first printed book on cryptology. He invented a steganographic cipher in which each letter was represented as a word taken from a succession of

columns. The resulting series of words would be a legitimate prayer. The advantage of steganography over cryptography is it doesn't attract attention towards the secret message. Modern digital applications include concealing messages within the lowest bits of noisy images or sound files. Steganography can be used for digital watermarking, where a message is hidden in an image such that it enables us to verify the source.

LSB bit encryption method involves the LSB of some or all the bytes inside an image being replaced with bits of the secret message.

For example, a grid of three pixels of a 24- bit image can be as follows:

01011101 00100010 11010100

01101111 00011010 01010001

10010101 01010001 01110101

When the number **200** whose binary representation is **11001000**, is embedded into the LSB of this part of the image, the resulting grid is:

01011101 00100011 11010100

01101110 00011011 01010000

10010100 01010000 01110101

3 MECHANISM DESIGNED

RGB encryption involves the representation of an image in terms of three colour components, namely Red, Green and Blue. Each component is like a gray scale image. So these components can be coded separately and concatenated at the end to receive the original image. Steps:

- The plain image is divided into RGB components.
- The secret image is hidden in RGB components of cover image.
- For each corresponding RGB components in image and key, diffusion is done.
- Concatenate RGB layers with binary representation for each in the order RGB.

Phase I: Encryption

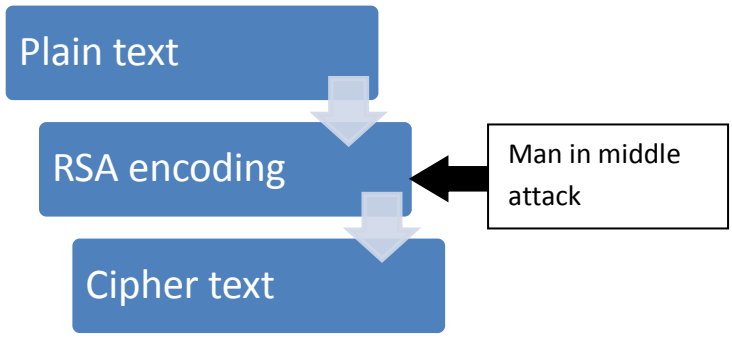
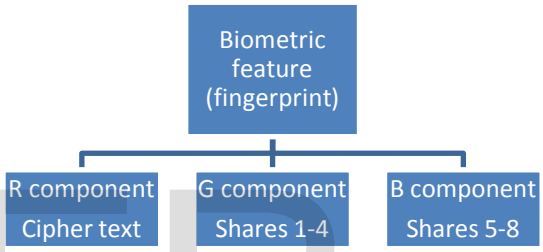


Figure 1: Encryption

Phase II: Component division



Cipher is hidden in the red component through LSB insertion.

Figure 2: Component division

Phase III: Sender's side

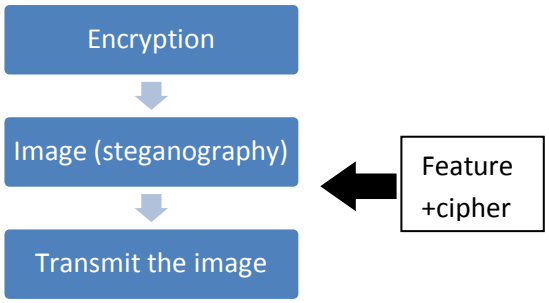


Figure 3: Algorithm at Sender side

Phase IV: Receiver's side

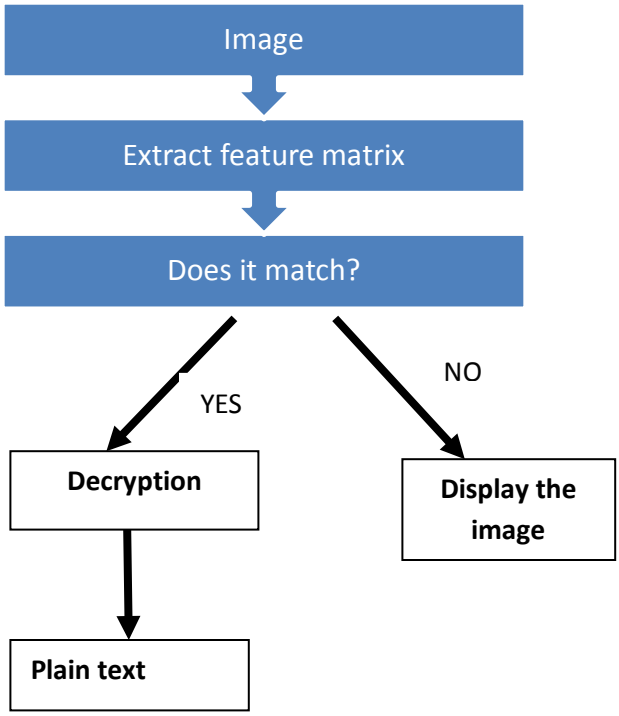


Figure 4: Algorithm at receiver side

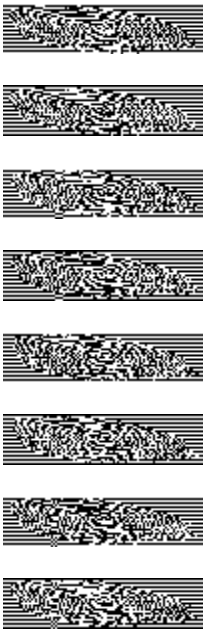


Figure 5: Shares Generated

4 Results

For carrying out implementation of the cryptographic mechanism designed we have used Matlab, which is a matrix-oriented programming language, which allows modulus operations too, so perfectly suits the basic structure of RSA algorithm. A hybrid mechanism using Image based steganography where biometric features are also been used for carrying out authentication and security has been designed. The plaintext after undergoing encryption through RSA is hidden in a colored image's RGB components and later after authentication it is successfully recovered. We have encrypted the plaintext and run the cipher thrice for showing how after successful authentication of recipient data is retrieved else its not disclosed. Here in we have generated 8 shares of the secret image using Manchester coding which is the fingerprint of the desired recipient is shown in figure 5.We have taken two fingerprints: fingerprint2 and fingerprint4. Then we have shown the result for unauthorized access where some other person tries to access the image then his fingerprints won't match and he would just be able to see the cover image only.

Later we have shown results for authorized access where the desired recipient accesses the cover image he gets the message hidden in it. Here PSNR of the covered image and watermarked image is infinity and data is retrieved if correlation between the fingerprints generated from shares and of the recipient is above 0.95.

fingerprint2 - fingerprint4

p=13

q=17

plaintext= coded message

The value of (N) is: 221

The public key (e) is: 5

The value of (Phi) is: 192

The private key (d) is: 77

Enter the message: coded message

Cipher Text of the entered Message:

Columns 1 through 9

216 76 172 186 172 2 96 186 98

Columns 10 through 13

98 54 103 186

comp =

0.3090

cipher =

Columns 1 through 9

216 76 172 186 172 2 96 186 98

Columns 10 through 13

98 54 103 186

Figure 6: Image shown in unauthorized access

Fingerprint2- fingerprint2

Figure 7: Cover image

Figure 8: Image hidden

Figure 9: Extracted image

Figure 10: RGB Components

p=13

q=11

The value of (N) is: 143

The public key (e) is: 7

The value of (Phi) is: 120

The private key (d)is: 103

Enter the message: coded text

Cipher Text of the entered Message:

Columns 1 through 9

44 45 100 62 100 98 129 62 120

Column 10

129

comp =

0.9670

Decrypted ASCII of Message:

Columns 1 through 9

99 111 100 101 100 32 116 101 120

Column 10

116

Decrypted Message is: coded text

fingerprint4- fingerprint4

p=13

q=11

The value of (N) is: 143

The public key (e) is: 7

The value of (Phi) is: 120

The private key (d)is: 103

Enter the message: coded text

Cipher Text of the entered Message:

Columns 1 through 9

44 45 100 62 100 98 129 62 120

Column 10

129

comp =

1

Decrypted ASCII of Message:

Columns 1 through 9

99 111 100 101 100 32 116 101 120

Column 10

116

Decrypted Message is: coded text

5 Conclusion and Future Scope

Traditional cryptographic methods relied on mathematical operations basically permutations and combinations which are now quite vulnerable to attacks but on integrating it with biometric and visual cryptographic modules we can make it more efficient and effective as compared to stand alone usage of

traditional cryptography. We have inculcated biometric and steganographic modules in well known cryptographic mechanism that is RSA which is a public key cipher so key sharing is also not a problem here as in case of symmetric cryptographic mechanisms like AES, IDEA etc. We have used Matlab for simulation and have encrypted and decrypted successfully. Future implementation may include 24 bit LSB insertion.

REFERENCES

[1] Mr. Vikas Tyagi, Mr. Atul Kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar , "Image steganography using least significant bit with cryptography", Journal of Global Research in Computer Science Volume 3, No. 3, March 2012.pp: 53-55

[2] "Cryptography and network security", Atul Kahate, second edition, Mc Graw hill companies.

[3] Nashwan A. Al-Romema, Abdulfatah S. Mashat, Ibrahim AlBidewi, "New chaos based image encryption scheme for RGB components of color image", Computer Science and Engineering 2012, vol. 2, No.5, pp: 77-85

[4] Jagdeep Verma, Dr.Vineeta Khemchandani ," A Visual Cryptographic Technique to Secure Image Shares" International Journal of Engineering Research and Applications IJERA, Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125.

[5] Kuang Tsan Lin , "Based on Binary Encoding Methods and Visual Cryptography Schemes to Hide Data", IIH-MSP '12 Proceedings of the 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing pp: 59-62

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

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

[8] 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.

[9] 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

[10] 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

[11] 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

[12] 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

[13] Raghunath S. Holambe, Ameya K. Naik ,"A Blind DCT Domain Digital Watermarking for Biometric Authentication"International Journal of Computer Applications (0975 -Volume 1 – No. 16 ,pp: 11-15

[14] Yambem Jina Chanu,Kh. Manglem Singh,"Image Steganography and Steganalysis: A Survey"International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012, pp: 2-11.