Image Based Stenographic & Cryptographic Process of Hiding Data

Ramsagar Tripathi[1], Purbani Kar[2]
[1]*VirtusaPolaris Seepz*
[2]*NIT Agartala*

Abstract- **In many organizations like FBI and RAWshare confidential and important data on any network. Hackers are always in wait for it. They hack the data and use it for their benefit. These peoples try to use these data to harm someone, they sale these important data to enemy countries. In either case, message sender or receiver has to pay the price. To protect from these undesirable acts, we can use Steganography and cryptography together to ensure security of the message. One of the most efficient and secure algorithms is RSA Algorithm for converting text message to cipher text. Steganography is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message and Cryptography is a mechanism to convert message or data in non readable form. In this paper, a methodology for digital image authentication using digital signature is proposed. The hash of the original message is taken and is encrypted by RSA. The digital signature obtained is stored on an location. Digital signature is checked with the decryption side signature and its checked by comparing both signatures and autheticity can be proved by this method.**

Index Terms- **LSB Steganography, RSA, Digital Signature, Histogram.**

I. INTRODUCTION

The widespread use of internet for communication has increased the attacks to users. The security of information is an important issue related to privacy and safety during storage and communication.[1] Cryptography and Steganography are two popular ways of sending vital information in a secret way. Cryptography is the method of converting plaintext into cipher text. The messages are converted into an encrypted format using a key and then this cipher text is hidden into an image, audio or video file according to the user's choice. The encryption is done using RSA algorithm with the use LSB Steganographic technique for hiding the data and also Digital Signature used for checking the authenticity of data.

II. TECHNIQUES USED

A. RSA Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasnt declassified until 1997. A user of RSA creates and then publishes the product of two large prime numbers, along withan auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

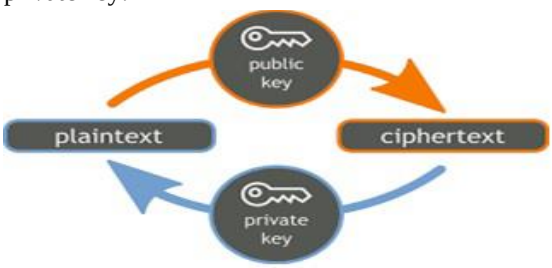

Fig1: RSA System

B. LSB Steganography

The least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. As an example, suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed).

10010101 00001100 11001000
10010111 00001110 11001011
10011111 00010000 11001010

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. The human eye cannot perceive these changes - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the LSB without noticing the difference.

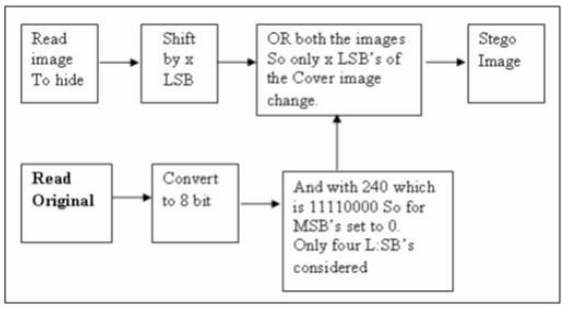

Fig2: LSB Steganography

C. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. The RSA digital signature scheme applies the sender's private key to a message to generate a signature; see Figure 1. The signature can then be verified by applying the corresponding public key to the message and the signature through the verification process, providing either a valid or invalid result. These two operations sign and verify comprise the RSA digital signature scheme.[2]

A digital signature scheme typically consists of three algorithms;

- A key generation algorithm that selects a private key uniformly at random from a set ofpossible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

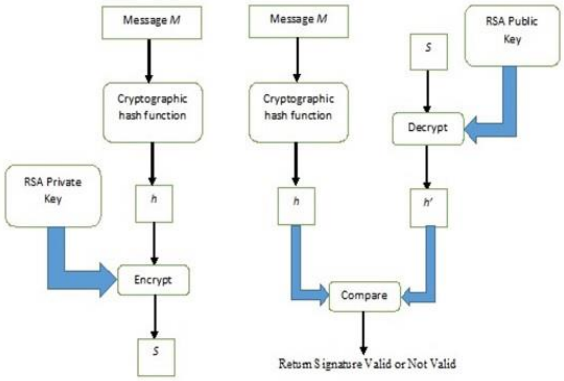

Fig3: Digital Signature

.III. PROPOSED METHOD

- This project using steganographic algorithms with RSA cryptographic algorithms.
- Digital signature can be also used for checking the authenticity of data.
- The message is transformed into a cipher data using a key, concealed into another cover data using Steganography by converting it into an intermediate encrypted and message with the help of RSA algorithms.
- For digital signature we can used the receiver's private key for conceal the message digest by taking the hash of the message and encrypted it with the sender's private key.
- At the receivers side we use sender's public key for fetch the signature and verify it with our senders side signature.
- The proposed method thus achieves a high degree of security, confidentiality and authentication for information.

A. In Encryption Section

- Firstly user have to write their message which he want to hide in the image.
- User have two choices they can choose his own RSA keys or automatically system can generate the keys.
- User will choose Public key for obtaining the Cipher Text of the message.
- User will press Steganography button for hiding the message in the image.
- A new concept Digital Signature has also implemented here for checking the Authentication of the message so user have to get the hash code of the message by using the Original message and RSA Private key obtained before encrypting the message.

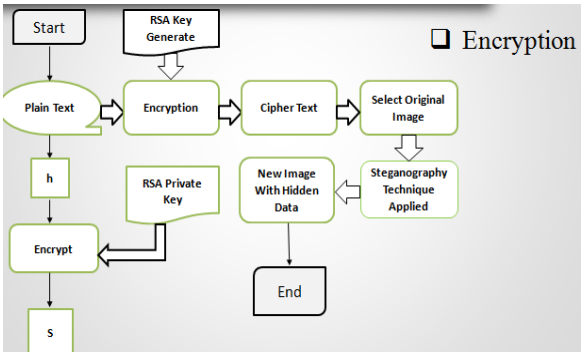

Fig4: Flow diagram for Encryption

B. In Decryption Section

- Here you have to select your Stego image first.
- Then click on Get Hidden Data button for obtaining the Cipher Text.
- Now browse your RSA Private Key for decrypting the original message.
- After getting the Original Data You have to match your Digital Signature.
- Now choose your RSA Public Key and your previously creates message Digest and click on Verify button for checking the Authenticity of message.

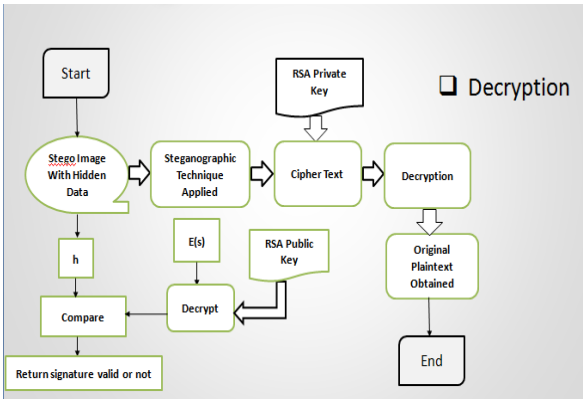

Fig4: Flow diagram for Decryption

IV. PERFORMANCE AND RESULTS

Steganography LSB method will be used for Hide the data in the image so the two images are:

Fig5: Original Image

Figure 6: Stego Image

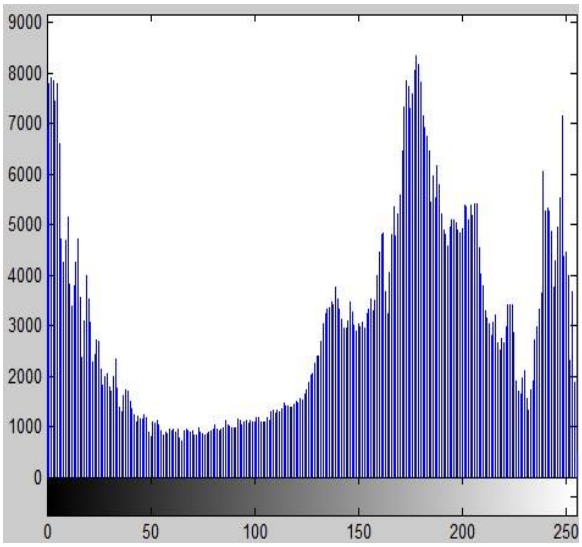

Figure 7:Penguins Histogram

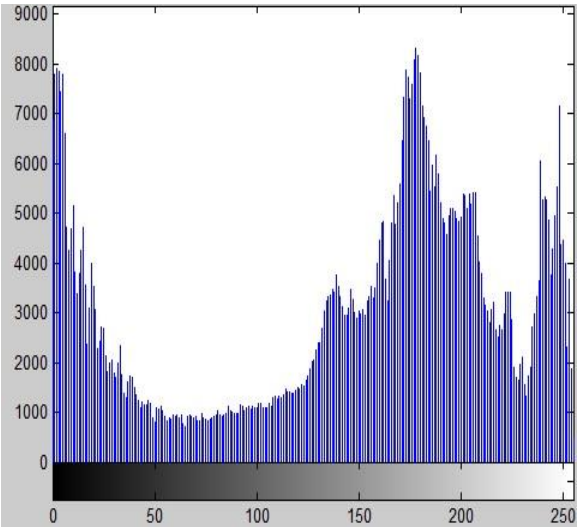

Figure 8:Penguins Stego Histogram

V. CONCLUSION

The proposed system has discussed implementation of securely using least significant bit manipulation based steganography that uses the RSA algorithm and Digital Signature technique. It can be concluded that when normal image security using steganographic and visual cryptographic technique is applied, the decryption of the encoded authenticated data becomes a cumbersome effort. The security features of the steganographic technique are highly optimized using the least significant bit manipulation along with RSA algorithm and Digital Signature. The proposed system yield an optimal grey scale output making it more efficient in real world applications and can withstand RS attack .The technique of steganography using visual cryptography in images has its scope on transmission of data in highly secured manner through audio streams and video streams. This is accomplished by encoding the audio data using steganography and cryptography technique in the audio streams and adopting the same technique to send the data in audio format, text format or image format in video streams. The technique in audio streams and images is best utilized in sending the data in video streams.

REFERENCES

[1] Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar, Enhance Security in Steganography with cryptography,(IJARCCE8C) International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014.

[2] Shahzad Alam, Amir Jamil, Ankur Saldhi, Musheer Ahmad, Digital Image Authentication and Encryption using Digital Signature,(ICACEA) International Conference on Advances in Computer Engineering and Applications,2015.

[3] Shamim Ahmed Laskar and Kattamanchi Hemachandran, Secure data transmission using steganography and encryption technique, (IJCIS) International Journal on Cryptography and Information Security, Vol.2, No.3, September 2012

[4] Tsutomu Matsumoto, Junji Shikata, Authenticated Encryption and Steganography in Unconditional Security Setting.