WWJMRD 2017; 3(10): 54-57
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Isiaka O. Salman
Computer Science Department, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin, Kwara State, Nigeria

Yusuf I. Tajudeen
Curl Links Technologies, Sulu-Gambari Road, Ilorin, Kwara State, Nigeria

Saka T. Olarewaju
Computer Science Department, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin, Kwara State, Nigeria

Correspondence:
Isiaka O. Salman
Computer Science Department, Institute of Information and Communication Technology, Kwara State Polytechnic, Ilorin, Kwara State, Nigeria

Secret Image Transmission with Visual Cryptography and Steganography Techniques

Isiaka O. Salman, Yusuf I. Tajudeen, Saka T. Olarewaju

Abstract
The need to develop new encryption schemes comes from the fact that traditional encryption schemes for messages are not suitable for multimedia data stream. Valuable multimedia content such as digital images, however, is vulnerable to unauthorized access while in storage and during transmission over a network. A new steganography algorithm is presented for hiding a secret image in a cover image. A fundamental task in many image processing applications is the visual evaluation of a distorted image. The scheme image Cryptography is used to encrypt an image or document by breaking into shares. In order to take the advantage of this property, the third party can recover the secret image if the shares of secret image are passing in sequence over a network. This paper presents an approach to encrypt image using Cryptography (2, 2) scheme for easy transmission over network. The aim of this paper is not only to show the efficiency in hiding the attributes with better cover image selection using steganography technique but also presents better image encryption with visual cryptography scheme for secured and effective image transmission over internet.

Keywords: Data Stream, Steganography Technique, Visual Cryptography Scheme, Encryption, Image Transmission

Introduction
Security is probably the most challenging and needed property in today's technological era. Many organizations have spent tremendous amount of money just to acquire this property for all their related projects. Without security, the data of any organization or a single unit is under threat of getting misplaced or completely taken out from existence. Such is the case with image transmission over network. Its security analysis is performed through a special method known as visual cryptography and steganography.

Visual cryptography known for its security uses the method of encryption to separate one image into many consecutive images. Advantage of visual cryptography is that it provides the user with decryption of code which does not require any complex computation. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into *n* shares so that only someone with all *n* shares could decrypt the image, while any *n* - 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all *n* shares were overlaid, the original image would appear. In its basic concepts, visual cryptography works in such a way that an image is split up into shares which look like white noise, but when those shares are overlaid they reveal the hidden image.

Steganographic techniques have been the most successful in supporting hiding of critical information in ways that prevent the detection of hidden messages. The techniques employ colour composition, luminance, unusual sorting of colour palettes, exaggerated noise, relationship between colour indices etc. The main objectives of the security or steganographic algorithms are to provide confidentiality, data integrity and authentication.

Applications for such a data-hiding scheme include in-band captioning, covert communication, image tamper proofing, authentication, embedded control, and revision tracking. As data security is proving to be one of the foremost concerns for transmitting over a local area network, across the Internet or any distribution system. Most steganographic techniques proceed in such a way that the data which has to be hidden inside an image or any other medium like audio, video etc, is broken down into smaller pieces and they are inserted into appropriate locations in the medium in order to hide them (Venkatraman, Marcin & Ajith 2004).

Cryptography and Steganography have been for a long time. Earlier a message was cipher using cryptography and sent to recipient, although it was secure approach yet it was visible message during transmission. Cryptography is the enciphering and deciphering of data and information with secret code. Visual cryptography uses the same concept with only difference that it is applied to images. Visual cryptography can also be deceiving to the inexperienced eye, in such a way that it would look like an image of random noise or bad art depending on the individual's experience. To make it invisible message next they applied steganographic method. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed. Steganography can avoid such policies to pass message covertly. Steganography is the technique in which messages, images, or files are confidentially stored inside other files or images. Steganography is indeed not a new concept; it dates back many millennia when messages used to be hidden on things of everyday use such as carvings or coded messages in letters or even using different watermark and other objects. The more recent use of this concept emerged.

The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal (Joshua, Soni & Bobate, 2014). Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

So far that numerous algorithms have been proposed in recent year in the fields of steganography and visual cryptography with the goals of securing messages, visual cryptography has the problem of revealing the existence of the hidden data whereas steganography hides the existence of hidden data. The research suggests by first encrypting the image in shares using visual cryptography and then hides the shares into images or audio files using steganography for easy transmission over network.

Methodology

This paper work will be divided into three segments/processes as thus:

1. Encryption process
2. Encoding and embedding process
3. Decryption and decoding process

Encryption Process

The encryption process takes the message to transmit as input and also takes the key for encryption and performs the encryption using RSA algorithm and produces the output as encrypted message. This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.

The RSA algorithm uses binary key that are several hundred bits long, typically 512 bits. RSA takes a binary block of plain text of length smaller than the key length and produces a cipher text that is the same length of the key. Suppose P is an integer that corresponds to a block of plain text. RSA encrypts P as follows

$C=P^e \pmod n$

Encoding and Embedding Process

This process takes the encrypted text as input. The RGB components of the image are extracted which is fed to the fitness function stage. Random selection function selects the pixels from the population randomly and provides the selected pixels as the input to the next stage. The pixels are selected by the genetic algorithm based on the threshold value determined by average value of pixels. In the next stage the message data bits are hidden in the selected pixels.

Stamping Algorithm

The simplest steganography technique algorithm employed in this paper is the stamping algorithm. This algorithm embeds the encrypted share with the covering image. For that, the shares can be divided into the blocks which contain the sub pixels each. Steps to embed encrypted shares in the covering image using stamping algorithm is as follows:

INPUT: Shares and covering images
OUTPUT: Embedded image
METHOD: Procedure Embedding (shares, cover images)
STEP 1: Calculate the collection of pixel for shares, cover images and secret image in coordinate (x,y)
STEP 2: Calculate required amount of cover pixels in shares in black and white region of the secret image
STEP 3: Calculate the amount of black pixels overlapped at coordinate (x,y)
STEP 4: Set the indicator for coordinate to 0 i.e., available for stamping cover pixel.
STEP 5: Add cover pixels on selected coordinates (x,y) of shares. The black pixels will be added on candidate coordinate (x,y) of share that has a white pixel on it.
STEP 6: Repeat Step 3 to Step 5 until all require cover pixels are stamped on shares

Visual Cryptography Technique

The basic idea of Visual Cryptography (2, 2) scheme is to create two shares, S1 and S2, consisting of exactly two pixels for each pixel in the binary image. Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process (Rohith & Vinay, 2012; Manisha, Sherekar & Thakare 2015). The four sub pixels are generated from a pixel of the secret image in a way that two sub pixels are white and two sub pixels are black. By superimposing the two shared sub pixels, the two participants can recover the

secret pixel. Pseudo code of share generation scheme is given below. Based on pixel bit and random sequence bit, share 1 and share 2 will be generated.

```
For i = 1 to Size of the image
    If (pixel i = 1)
        If (random_bit =1)
            Share 1 = [1 0]
            Share 2 = [1 0]
        Else
            Share 1 = [0 1]
            Share 2 = [0 1]
        If (random_bit = 1)
            Share 1 = [1 0]
            Share 2 = [0 1]
        Else
            Share 1 = [0 1]
            Share 2 = [1 0]
    End
```

Decryption and Decoding Process

This process takes the watermarked image as the input. The pixels which contain the message bits are detected and the data within the pixels are extracted. The extracted bits contain the message digest. The extracted bits are decrypted and the message is separated from the message digest. Decryption process is done by using RSA algorithm.

$C^d \pmod n = (P^e)^d \pmod n = P^{de} \pmod n = P \pmod n = P$

Steps to extract the embedded text Input: watermarked image

Begin:

Step 1: Get the pixel value from image and get the LSB value from the pixel

Lsb<-getbit(pixel value)

Step 2: check the lsb value

Step 3: Get the bits from the pixel value from the lsb bit

Step 4: Combine all the bits got from the lsb bit and from the text

End

Output: The text hidden in the image

Result and Discussion

The proposed scheme is designed with two sides i.e. sender side and destination side. At sender side, the scheme first encrypts the message with RSA algorithm. First we have generated the key for RSA and then we perform the encryption using public key. The encrypted message are then embedded in covering image using Stamping algorithm in order to secure and protect the message from the vicious third party. The basic Visual Cryptography (2, 2) scheme is then apply on secret image to generate the shares of pixels which will be easier to be transported over network. At destination side, secret shares are first extracted from covering image, then using RSA decryption algorithm, we again convert the encrypted messages into their actual form, which were encrypted at the sender side and then stacked to reveal the binary image. The final stage was the decoding or conversion of binary image to the actual secret image using HEX function.

The flowchart for the implementation of the proposed secret image transmission over network using Visual Cryptography (2, 2) and Stamping Algorithm is shown in figure 1.0.

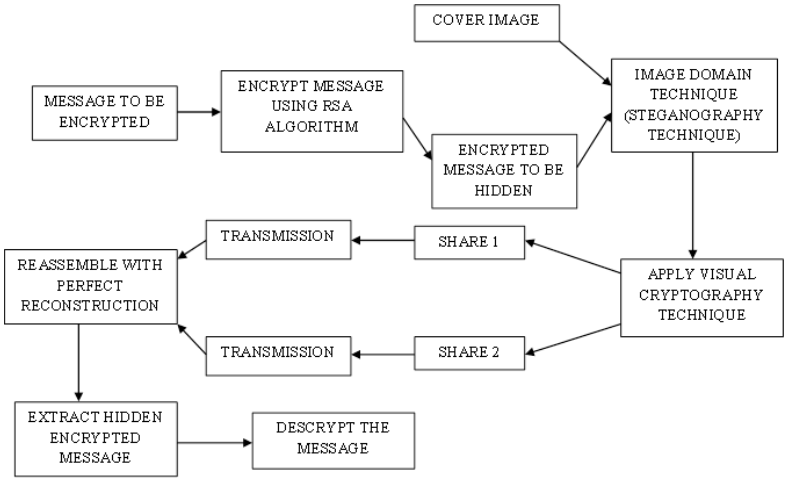

Fig. 1.0: Proposed Flowchart for Secret Image Transmission over Network using Visual Cryptography and Steganography Techniques

Conclusion

The use of stamping algorithm for steganography technique and RSA algorithm for encryption and decryption purposes alongside visual cryptography is strong concepts that add a lot of challenges to detecting such hidden and encrypted message. The paper proposed uses one of the strong algorithms of steganography technique i.e. stamping algorithm to hide data inside an cover image, which was then split into shares with a strong visual cryptography method. The shares would then be effectely transmitted over the network after which, at the destination side, the shares would be re-assembled or decoded to reconstruct the original image that would then reveal image which still contains the hidden message. So the receiver would be able to extract the hidden message from the revealed image. This algorithm cannot exist without having a perfect reconstruction property in the visual cryptography method. The reason for that is that if the reconstruction process or even the encryption process alters the image message, then it would consequently alter the hidden message which would make it impossible to extract the hidden message from the revealed image.

References

1. Anjney P. & Subhranil S. (2016). “Applications and Usage of Visual Cryptography: A Review”. 5 International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and

Future Directions), Sep. 7-9, 2016, AIIT, Amity University Uttar Pradesh, Noida, India
2. Aoki, N. (2009). "A lossless steganography technique for G.711 telephony speech". APSIPA Annual Summit and Conference (APSIPA ASC 2009), Sapporo, Japan, pp. 274-277
3. George A., Jeffrey M. & Roman V.Y. (2010). "Steganography and Visual Cryptography in Computer Forensics". Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering
4. Joshua D. A., Soni C. &. Bobate R.V (2014). "Steganography and Visual Cryptography in Videos for Secure Communication". International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
5. Néelima. G. & Ratna-Raju P.D. (2011). "An Introduction to Different Types of Visual Cryptography Schemes". International Journal of Science and Advanced Technology (ISSN 2221-8386)
6. Pavithra V., Manjunath C.R. & Sandeep.K (2013). "Integration of Steganography and Visual Cryptography for Authenticity". International Journal of Emerging Technology and Advanced Engineering; Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6)
7. Rajesh K.N., Manikandan G., Bala K.R., Raajan N.R. & Sairam N. (2017). "A Reversible Visual Cryptography Technique for Color Images using Galois Field Arithmetic". *Biomedical Research-India; 28 (5): 2036-2039. ISSN 0970-938X* www.biomedres.info.
8. Venkatraman S., Marcin P. & Ajith A. (2004). "Significance of Steganography on Data Security". Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) 0-7695-2108-8/04 $ 20.00 © 2004 IEEE