RESEARCH ARTICLE OPEN ACCESS

STEGANOGRAPHY and VISUAL CRYPTOGRAPHY in VIDEOS for SECURE COMMUNICATION.

Joshua D Augustine
M.Tech. Scholar
P.I.E.T. Nagpur, India
joshua.aug@gmail.com

Prof. Soni Chaturvedi
Asst. Prof. ,E&C
P.I.E.T. Nagpur,India
soni2569@gmail.com

Prof. R.V. Bobate
Asst. Prof. ,E&C
P.I.E.T. Nagpur, India
ranjit.vb@gmail.com

Abstract—
Recently, numerous novel algorithms were planned within the fields of steganographyand visual cryptography with the goals of rising security, dependability, and potency. This paper discusses and compares both the methodologies. Some similarities and variations are provided, additionally to discussing a number of the most effective acknowledged algorithms for both. Lastly a possibility of combining them for an even more advanced, 'secured communication' in videos which is a stream of imaged in which these encryption techniques are implemented. The advantages of using videos over images are discussed in this paper as well.

Keywords- Visual Cryptography, Steganography, Data Hiding, Secured Communication, Shamir's Secret Sharing, Least significant Bit Replacement: Technique

I. INTRODUCTION

Steganography is the techniquein which messages, images, or files are confidentially stored inside otherfiles or images. Steganography is indeed not a new concept; it dates back many millennia whenmessages used to be hidden on things of everyday use such as carvings or coded messages in letters or even using different watermarkand other objects. The more recent use of this concept emerged with the dawn of the digital world.Experiments have shown that data can be hidden in many ways inside different types of digital data or files. The mainbenefit of steganography is that the hidden data (payload) is not expected by the investigators who get to examine the computerdata. The person sending the hidden data and the person meant to receive the data are informed aboutit; but to everyone else, the object containing the hidden data just seems like an everyday normal object with no other meaning.

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 besomewhat deceiving to the inexperienced eye, in such a way that, if an image share were to fall into the wronghands, it would look like an image of random noise or bad art depending on the individual's experience [1].

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 Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

II. IMAGE STEGANOGRAPHY

Steganography is an area in which many studies and intensive research have been carried out. There are severaldifferent methods and algorithms of hiding data in different types of files. One example of an advanced hidingtechnique in images is using image layers. This method divides the original image into several blocks, and thencreates layers for each block of the binary values of pixels as matrices [1]. The second step to hide the secret bits is tosearch within these layers' rows and columns and try to find the best match between the binary value of the pixelthat is being hidden and the binary value of the pixel where we want to hide it. So for example, if the value of thepixel that we want to hide is '1001', but we did not find a '1001' in any rows or columns of the binary layers of theoriginal image, but we did find a '1000' then this is selected as the closest match and that secret pixel is hiddenthere.This method hides less data per block, it only hides 1 byte in an 8 x 8 pixels block whereas other methods likethe LSB (Least Significant Bit) matching revisited method hides 1 bit in every pixel[1]. So this method hides lessdata per block which increases performance and sustains a better image quality. The significant thing about thismethod is that it doesn't rely on hiding data in the LSB of pixel values, but tries to find the best secret pixel –original image layer pixel binary value match in higher layers of the image thus preserving the quality of the imagewhich makes it somewhat resistant to steganalysis. The Dynamic Compensation LSB Steganography method provides an even higher resistance to steganalysis and histogram analysis. This method hides data in the LSB of the original image pixels, and then compensatesdynamically on the resultant image [1]

III. VISUAL CRYPTOGRAPHY

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 MoniNaor 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 basicconcepts, 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. Many studies have been performed in the area ofvisual cryptography and several algorithms have been developed.One interesting visual cryptography method is the (t,n) Threshold Image Hiding Scheme[2]. This method hidesa secret image into 'n' number of cover images, and can be recovered if't' number of cover images are available.The hidden image can be up to 512 colours with a size as big as that of the cover images. This method uses Lagrangeinterpolating polynomial, MD5 hashing, and RSA signature to encrypt the image to be hidden. The interestingthing about this algorithm is that during extraction of the hidden image from the cover images, it implements a cheatattack check where it checks whether these cover images are the same as the ones used to hide the data. If that checkfails then the extraction of data is aborted [2]. The authors of this method do not mention anything about the quality ofthe hidden image after extraction and how similar it is to the original image, although they do mention that the coverimages used in their experiment are of relatively good quality with an average PSNR (Peaks of the signal-to-noiseratio) value of 31.34.Another visual cryptography algorithm is the Image Size Invariant Visual Cryptography [3]. This method hidestwo-tone secret image and splits it into binary transparencies which look like random noise images. Once thosetransparencies are stacked on top of each other, the secret image is revealed. The secret image can also bereconstructed by XOR computations of the transparencies. This algorithm is based on the conventional VSS (VisualSecret Sharing) method.The JVW method is one that uses the concept of watermarking and visual cryptography jointly. Since theDHCED (Data Hiding in Halftone Image by Conjugate Error Diffusion) method cannot prevent the secret imagefrom being extracted with only one of the shares, JVW was proposed to overcome that issue. JVW consists oftwo main steps; the first is to add some noise to the original multi-tone image [3]. Introducing random noise to theoriginal image breaks the direct correlation between it and the share images without affecting the perceptual quality,which means that when we overlay the shares we will still be able to identify the original image. The second step isto modify the DHCED algorithm to accommodate two halftone images instead of just one. An interesting point ofthis algorithm is that it does not reveal the secret image even if one has the original image and one of the shares;both shares have to be present to reveal the secret image [3].Next the RIVC (Region Incrementing Visual Cryptography) method is discussed. In RIVC, the originalimage is sectioned into 'n' number of secrets and then 'n+1' number of shares are then created. Any 'n' number ofshares stacked would reveal 'n- 1' number of secrets [3]. The advantage to this method is that a user can pick whichregion of the secret image to assign to a secrecy level, and thus it makes it flexible and accommodating to userpreferences. As this method may not seem to be as secure as other methods because of the fact that some levels ofsecrecy can still be revealed even if one doesn't have all the shares, it is hard for the person who is trying to revealthe secret data to know if the shares that they have are all the shares or if they're missing any. So if someone has 3out of 5 shares and sees some data revealed, they may think that they've found the secret and stop looking for theother two. But if someone is using this method to hide a certain secret in a certain level, but decides to create othersecrets as decoy, this doesn't guarantee the hider that others won't be able to reveal that secret if they happen toobtain the right shares. This is definitely an interesting method because it can be used in many ways and it ischallenging to tell which shares reveal the real secret and which shares reveal decoy secrets.

IV. DESIGN DETAILS

First we start with an image (decompiled from video) that contains steganography. i.e data is incorporated within the image pixels. The image is then broken into two or more images printed on transparencies. Each transparency should have some, but not all, of the steganography-encoded pixels of the original image. When the transparencies are combined, the image will be whole, and that image can then be decoded the steganography decryption program.

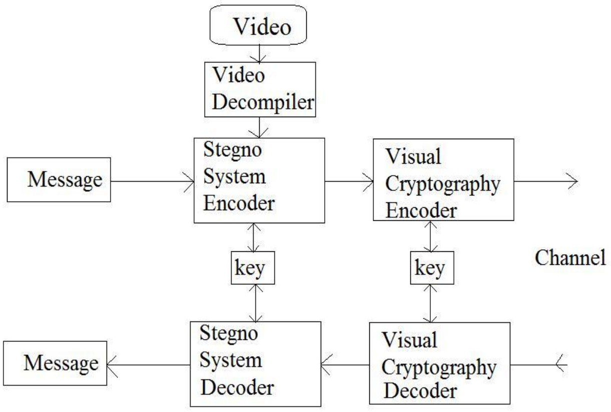


Fig 1

Video and its utilization:

The Input video gives us a valid and safe carrier for the Information that needs to be transferred. The decompiler, decompiles the input video to a stream of images and numbers them. Blaze Media is a very famous windows decompiler Message:

The information to be transferred is sent through other input of stegno-encoder.

Stegno-encoder: The stegno Encoder uses the LSB Technique.

Least significant Bit Replacement: Technique: In imagesteganography the majority information concealing techniques try andalter insignificant info within the cover image. Leastsignificant bit (LSB) insertion could be a common, simpleapproach to embedding info during a cover image. Forinstance, an easy theme planned, is to put theembedding information at significant vital bit (LSB) of everypixel within the cover image [7] . The altered image iscalled stego-image. altering LSB doesn't modify thequality of image to human perception however this scheme issensitive a spread of image process attacks likecompression, cropping etc. we are going to be accentuation a lot ofon this method for the assorted image formats.

The other option in using stegno encoder is the MSB techinique

The moderate significant bits of each pixel in the cover image can be used to embed the secret message. This method improves sensitivity to modification,

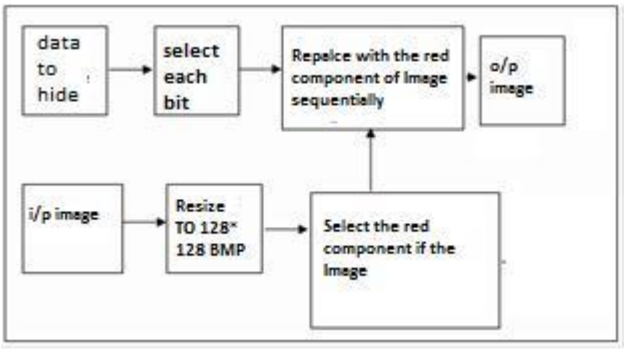

data to hide
select each bit
Repelce with the red component of Image sequentially
o/p image
i/p image
Resize TO 128* 128 BMP
Select the red component if the Image

Fig 2

Algorithm for Hiding (Steganography)

1. Read the original image and the image which is to be hidden in the original image
2. Select the red component of the image and replace its pixels with the data to hid

Decoding Process

1. Check all the images for data
2. Extract the data from the red component

Visual cryptography Encoder/Decoder

In cryptography we use Shamir's Secret Sharing which is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.i.eShamir has introduced a simple and elegant way to split a secret Aε 2 GF(2^l) into n shares such that no tuple of shares withcardinality lower than a so-called threshold d < n depends on A[7]

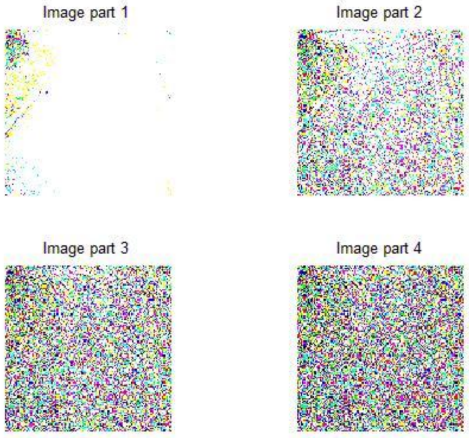


Fig 3 Visual crypography

Formally, our goal is to divide some data D (e.g., the safe combination) into n pieces D1…,Dn, insuch a way that: Knowledge of any k, or more Di, pieces makes D,easily computable.

Knowledge of any k-1, or fewer Di pieces leaves D, completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called (k,n), threshold scheme. If k=n then all participants are required to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k Points to define a polynomial of degree k-1[6].

Suppose we want to use a(k,n),threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size 0 < k≤ n < P where P is a prime number.

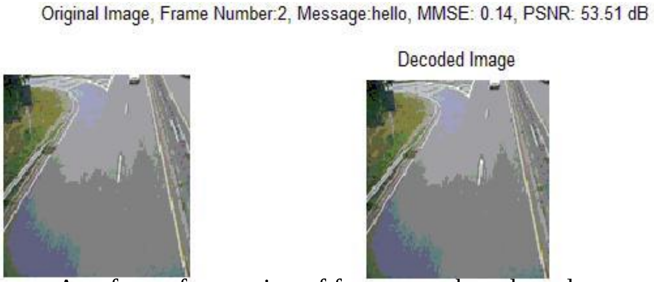
Choose at random k-1 coefficients a1,…,a{k-1} in F, and let

a0=S, Build the polynomial $f(x)=a0+a1x+a2x^2+a3x^3+000+a\{k-1\}x^{\{k-1\}}$. Let us construct any n points out of it, for instance set i=1,

…n to retrieveleft(i,f(i)), Every participant is given a point (a pair of input to the polynomial and output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation and the secret is the constant term a0[6]

V. CONCLUSION:

Providing both stegnography and cryptography improvises security of the communication also since video already consist of stream of expectedly the system should have a high psnr as shown below.



Original Image, Frame Number:2, Message:hello, MMSE: 0.14, PSNR: 53.51 dB

Decoded Image

Any frame from string of frames can be selected or set of frames for large messages.

REFERENCES:

[1.] George Abboud Jeffrey Marean Roman V. Yampolskiy “Steganography and Visual Cryptography in Computer Forensics”

[2.] F. Ming Sun and O. C. Au, "Data hiding in halftone images by conjugate error diffusion," in *Circuits and Systems, 2003. ISCAS '03.Proceedings of the 2003 International Symposium on*, 2003, pp. II-920-II-923 vol.2.

[3.] F. Ming Sun and O. C. Au, "Joint visual cryptography and watermarking," in *Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on*, 2004, pp. 975-978 Vol.2.

[4.] C. Chin-Chen and L. Iuon-Chang, "A new (t, n) threshold image hiding scheme for sharing a secret color image," in

[5.] *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003, pp. 196-202 vol.1

[6.] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, “Implementation of LSB Steganography and itsEvaluation for Various File Formats”.

[7.] Wikipedia - Shamir's Secret Sharing Jean-SebastienCoron, Emmanuel Prou , and Thomas Roche, “On the Use of Shamir's Secret Sharing AgainstSide-Channel Analysis”

[8.] A. Swathi , Dr. S.A.K Jilani, “Video Steganography by LSB Substitution Using Different Polynomial Equations”