ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (58-62), Month: January - March 2015, Available at: www.researchpublish.com

Survey Paper on Multilevel Security Using VC and BPCS

[1,] Rewa Ambar, [2]Radhika Deshpande, [3]Abhaya Doshi, [4]Abhaya Renuse

[1,2,3,4]Department of CE, University of Pune, India

***Abstract*: Internet communication has become an integral part of the infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. Such secrete communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases on down to large percentage of everyday email. In reality the Internet is not a secure medium. We are suggesting Visual Cryptography approach which is simple, fast and provide privacy protection when sharing sensitive financial documents over the Internet. In Visual Cryptography financial document is represented as bit map file, and expands it into two or more encoded file shares. These shares can be transferred to the recipients via electronic mail or electronic file transfer process. These shares can be transferred to the recipients in stego image using Bit Plane Complexity Steganography technology via electronic mail or electronic file transfer process.**

The Bit Plane Complexity Steganography technique allows hiding large data into cover image, which allows hiding large secret information into cover image. The use of Steganography for data transfer is added security during data transfer. Moreover, the final image can be obtained only when desired numbers of shares combined together at receiving side. The combined use of Visual Cryptography and BPCS Steganography provides added security to confidential documents during transfer over internet.[4]

***Keywords:* VC (Visual Cryptography), BPCS (Bit Plane Complexity Segmentation), SI (Secret Image), Steganography, Encryption, Decryption.**

I. INTRODUCTION

Security is one of the most important factor for transferring different kinds of important documents. Internet is one of the widely used media to transfer documents. Such secrete documents contains information about bank transfers, corporate communications, and credit card purchases on down to large percentage of everyday email. In reality the Internet is not a secure medium, because one can easily access confidential information in document where internet is transfer medium .

In traditional cryptography variety of algorithm such as RSA, DES, Triple DES,AES IDEA etc are used for encryption to provide security. But these algorithms are complex and inefficient.

One of the most obvious limitations of using visual cryptography in the past was the problem of the decoded image containing an overall grey effect due to the leftover black sub pixels from encoding. This occurred because the decoded image is not an exact preproduction, but an expansion of the original, with extra black pixels. Black pixels in the original document remain black pixels in the decoded version, but white pixels become grey. This resulted in a loss of contrast to the entire image. The extra black sub pixels in the image cause the image to become distorted. This is unacceptable since the digits used in the financial documents must be clearly discernible.

Original image gets distorted while recovering it from shares using 'Traditional Visual Cryptography' this drawback is removed by this system. Example below shows demonstration:

In simple Steganography using 'LSB Replacement algorithm' we can hide at most 20-30 % of original data. It cannot support to hide large amount of data into images.[5]

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (58-62), Month: January - March 2015, Available at: www.researchpublish.com

II. VISUAL CRYPTOGRAPHY SCHEME

The algorithms used for visual cryptography methods are as follows:

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images .The way that the original image can be reveals only when both images are simultaneously available. The use of visual cryptography is explored to preserve the privacy of digital data (Image Passwords, QR code of the websites etc.).In this paper, visual cryptography for binary images used in QR code application and visual cryptography for colour images.[1]

There are two main steps of visual cryptography: share generation and extraction of original key image.

1) Algorithm of Share generation:

Step 1: Take the binary image (two tone image) as a key image.

Step 2: Divide the binary images in to two shares as shown in figure 1.

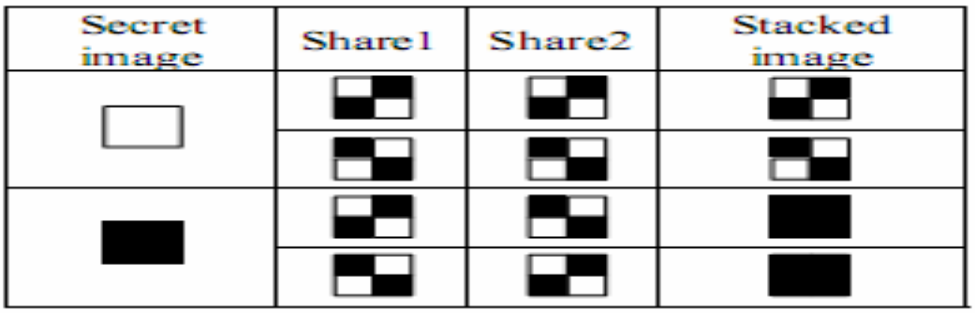

Fig. 1 VC(2,2) Schema[8]

Algorithm for reconstruction of original image:

Step 1: Take the two shares (Shares are random noise images).

Step 2: Overlap the two shares to get the original image. Overlapping is simple OR operation or EX-OR Operation

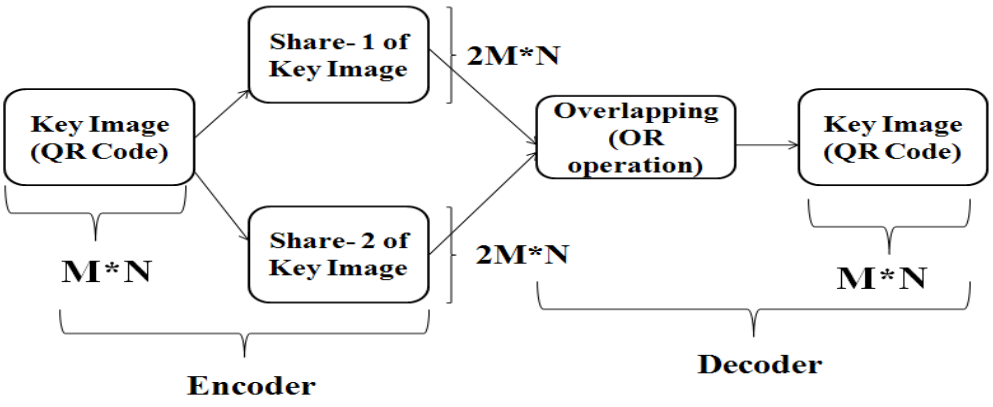

Fig.2 Block diagram of visual cryptography (2, 2) schema[8]

2) Visual Cryptography for colour images:

Algorithm for share generation:

Step 1: Take the colour image (RGB image).

Step 2: Take the number of shares ‘n’ and minimum number of shares ‘k’ to be required to reconstruct the final image, ‘k’ must be less than or equal to ‘n’

Step 3: Calculate reconstruction factor, Recons = (n-k) +1

Step 4: Select the one pixel from original image and convert it into 32 bit binary string

Step 5: take the 1st bit of binary string if it is 1 then in (n-k) +1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of pixel there will be 0. A random number generator is used to select (n-k) +1 number of shares. Repeat the same procedure for all bits in the 32 bit binary string to reproduce the pixel share.

Step 6: Apply the same procedure of all pixels as mentioned in step 5 to generate shares.

Algorithm for reconstruction of original image:

Step 1: Take any 'k' number of shares to generate original image.

Step 2: Take 1st pixel of each share then convert them into 32 bit binary string.

Step 3: Perform the OR operation on 32 bit string of all shares to get original image pixel. Repeat the same procedure for each pixel from share.

Step 4: Repeat the procedure mentioned in step 3 to get original image by overlapping all 'k' shares. Less than 'k' number of shares should not retrieve the original image [8].

The algorithms used in steganography method are as follows, the reversible data hiding algorithms used for steganography which gives perfect recovery of hidden data as well as cover image.

III. BPCS STEGANOGRAPHY

Existing methods can hide only 25% (or less) of the data amounts of the vessel. This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multi-valued image with the secret information. Our new BPCS Steganography uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel.

This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality.[8]

Here the actual steganography is performed. In our method we call a carrier image a carrier. It is a colour image in BMP file format, which hides (or, embeds) the secret information (files in any format). We segment each secret file to be embedded into a series of blocks having 8 bytes of data each. These blocks are regarded as 8 × 8 image patterns. We call such blocks the secret blocks. We embed these secret blocks into the vessel image using the following steps.

1. Convert the carrier image from PBC to CGC system i.e. convert file from any format into png format.
2. Segmentation on carrier image is performed i.e. each bit-plane of the carrier image into informative and noise-like regions by using a threshold value (α0).That means complexity of image is calculated.
3. Group the bytes of the secret file into a series of secret blocks.
4. If a block is less complex than the threshold (α0), then conjugate it to make it a more complex block.
5. The conjugated block must be more complex than α0.
6. Embed each secret block into the complex regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks) where maximum color changes are observed.
7. Convert the embedded dummy image from CGC back to PBC.[8]

We termed our Steganography "BPCS-Steganography," which stands for Bit-Plane Complexity Segmentation Steganography. We made an experimental system to investigate this technique in depth. The merits of BPCS-Steganography found by the experiments are as follows.

1. The information hiding capacity of a true color image is around 50%.
2. A sharpening operation on the dummy image increases the embedding capacity quite a bit.
3. Randomization of the secret data by a compression operation makes the embedded data more intangible.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (58-62), Month: January - March 2015, Available at: www.researchpublish.com

IV. FUSION TECHNIQUE

The multi-share crypt-stego authentication system uses both visual cryptography and steganography. There are two main components encoder and decoder. At the encoder side, key image is the input to visual cryptography stage which divides key image in to multiple shares. The output of visual cryptography stage is forwarded to steganography stage for hiding shares into cover image (stegoimage). At the decoder side, stegoimage is the input to reverse steganography stage for extraction of hidden shares. All output shares are forwarded to visual cryptography stage which overlaps all shares to generate key image. Then the output of decoder stage is checked with certain threshold to decide whether access is allowed or is denied for user.[8]

V. PROPOSED METHODOLOGY

Project Components:

1) The Encoder:

a) Input the key image to visual cryptography stage.

b) Divide the key image into multiple shares (for code application divide key image into two shares using visual cryptography for binary image and in banking application divide key image into multiple shares using visual cryptography for color images).

c) Hide share into cover images using reversible data hiding with histogram based difference expansion steganography techniques.[8]

2) The Decoder:

a) Input stego image to extraction stage i.e. reverse steganography technique.

b) Retrieve the share from stego image using extraction technique.

c) Pass shares to fusion step.

d) Overlap the shares in fusion stage i.e. reverse visual cryptography technique to get the key image.

e) Compare key image to original key image in comparison stage.

f) Check the output of comparison step with certain threshold and then decide whether access allowed or denied for user [8].

VI. WORK FLOW

In Visual Cryptography financial document is encrypted and then converted into as bit map file called secret Image. The secret image then expands it into two or more bit map file shares. These shares can be transferred to the recipients in stego image using BPCS Steganography technology.

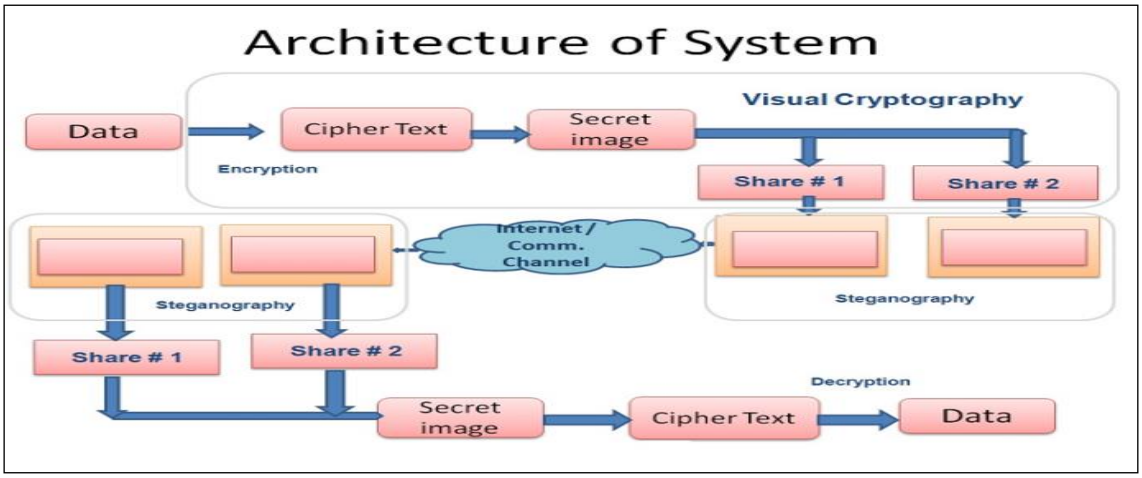

Fig.3 Architecture of System

VII. APPLICATIONS

1. Transfer Sensitive, Confidential Documents via unsecured medium like internet etc. Documents may be Banking Excel sheets which contains Account info etc.
2. Company Balance sheet Transfer one place (sites) to another places.
3. Transfer ATM Pin Code to user.
4. In Military Surveillance sharing Secrete information (like Secrete Message in groups, Passwords, Mission information).
5. Sharing Password for Online Polling System.
6. Sending personal information to another person via untrusted sources.[2] [3]

VIII. CONCLUSION

The objective of this paper is to demonstrate BPCS-Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans can not see any information in the bit-planes of a color image if it is very complex. We have specified the two techniques of BPCS one is web based BPCS and another is Improved BPCS technology.[5][6] Web Based technology guarantees secret Internet communication. This steganography is a very strong information security technique, especially when combined with encrypted embedded data. The technique of improved steganography text based on chaos and BPCS apply to text secret information, the design has good visual imperceptibility and high data embedding capacity, and furthermore, it has a great advantage in resisting the analysis of the steganalysis. By introducing chaos theory and RSA algorithm, it is convenient to test the performance of steganography, and the design has higher security and reliability.[7]

ACKNOWLEDGEMENT

We would like to take this opportunity to express my profound gratitude and deep regard to our project guide Prof. A.V. Dhumane, for his guidance, valuable feedback and for constant encouragement for the project. Working under him was extremely knowledgeable experience for us.

REFERENCES

[1] International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–047 Volume 1, Issue 1, 2010, PP-32-37

[2] Jessica Fridrich, Steganography in digital media, Technology and Engineering Journal.

[3] L. W.Hawkes, Yasinsac, C. Cline, an Application of Visual Cryptography To Financial Documents by Security and Assurance in Information Technology Laboratory.

[4] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai, and Y. P. Chu (2007). A multiple-level visual secret-sharing scheme without image size expansion. Information Sciences, 177(21), 4696-4710.

[5] Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique IJEST Vol. 2(9), 2010

[6] Steve Beaullieu, Jon Crissey, Ian Smith, BPCS Steganography, International Journal Of Engineering And Science ,Vol.3, Issue 2 (May 2013), PP 08-16 Issn(e): 2278-4721, Issn(p):2319-6483

[7] S.Mehta, K.Dhige, M.Jagtap ,Web Based BPCS Steganography, international journal of computer tecnology and entc engineering, volume 2, 2012, pg no 1

[8] Om Prasad Deshmukh Shifali Sonawane,International Joutnal Of Computer Science and mobile Computing, IJCSMC,Vol- 2,Feb 2013 ,pg no 80-90