International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Efficient Image Design Using Natural image based VSS Scheme by Different Image Media

Sreenivasa T V[1], M. N Ravikumar[2]

[1] *M.Tech (DE&CS) Student, E&C Department, Malnad College of Engineering, Karnataka, India*

[2] *Associate professor, E&C Department, Malnad College of Engineering, Karnataka, India*

Abstract - *The procedure that used to encodes a secret image into number of shares is called Visual Cryptography, with every member holding one or more shares. It can't uncover any data about the secret image that holds less than n offers. Stacking that each one of those shares uncovers the secret image and it can be perceived specifically by the human visual framework. We have distinctive sorts of mystery pictures those are pictures, photos, manually written archives and others. Visual Secret Sharing (VSS) plan means sharing and conveying mystery pictures. Ordinary visual cryptography experiences a pixel-development issue, or unmanageable quality issue for recouped pictures, and does not have a general way to deal with develop visual secret sharing plans for general access structures. The unaltered characteristic shares are different and harmless, therefore incredibly decreasing the transmission hazard issue.*

Key Words: Secret Image, Visual Cryptography, Visual secret sharing, Halftone Visual Cryptography, Conventional shares, Color image, Bitwise image, transmission risk, etc…

1. INTRODUCTION

Today's computer aided environment and rapidly growing technology trends safety to ours information is very important than ever. As technology trends increasing threat are also come in different form such as theft, fraud, viruses attack, information extortion etc. Several media reports frequently this kind of fraud stories and number of such cases are increasing exponentially. As this kind of attacks or information extortion continues people lost their confidence on their information only. To protect ourselves from these kind of attack there are many ways but carefulness is the most significant precautions to protect our information.

In this computer world, internet spread its network all around the world. Millions of internet users accessing required digital data via internet networks. The internet user can upload and download their information with less secure channels. The information which is uploaded and downloaded by internet user can be many types i.e. text, image, audio, video etc. any one of the form of information can be shared via internet. Cryptography is the one of the technique to secure our information in which a key is used to encrypt or encode our image information and same key is used while decrypting or decoding for information extraction.

Conventional visual secret sharing plans hide secret pictures in shares that are either imprinted on transparencies or are encoded and put away in a computerized structure. The shares can unmistakable as important pictures or commotion like pixels; however it will stimulate suspicion and rise the extent of interference danger amid transmission of the shares. Subsequently, visual secret sharing plans experience the ill effects of a transmission hazard issue for the mystery picture itself and for the clients who are all included in the visual secret sharing.

2. RELATED WORK

Visual cryptography is an image-based secret protection mechanism in which the decoding process is conducted by inspecting the stacked shares with the naked eye. In visual cryptography the image is divided two transparent images one transparent image, layer 1, which has pixels that all have a random state, which is 1 of the 6 possible states. Layer 2 is similar to layer 1, other than the pixels that should be black (which contains information) when overlapped. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlapped the areas with the similar states will look gray, and the all pixels areas with opposite states will be black.

We have various Visual Cryptography schemes those are:
1. (2, 2) Visual Cryptography Scheme.
2. (k, n) Visual Cryptography Scheme.
3. Halftone Visual Cryptography Scheme.

4. Visual Cryptography Scheme for Gray images.

The basic (2, 2) visual cryptography scheme contains of a secret message encrypted into two transparencies, one transparency representing the cipher text and the other acting as a secret key. Both transparencies appear to be random dots when inspected individually and provide no information about the original clear text. However, by carefully aligning the transparencies, the original secret message is reproduced. The actual decoding is accomplished by the human visual system.

Visual cryptography is an encryption technique where visual information (Image, Text etc.) gets encoded in such a way that decryption can be performed by human visual system without a complex decoding process. The beauty of the visual secret sharing scheme is in its decoding process where we can obtain secret images without any complex computation that is by using human visual system. But the encoding process needs cryptographic computation to divide the secret image into a number of parts that is let n parts or shares are obtained from image but at least a group of k shares out of n shares helps to get back the secret information, without k number of shares i.e. shares number is less than k we cannot obtain any information about secret image.

Halftone visual cryptography is a one of the type of cryptography in which secret image is encoded into shares which has different binary patterns. The secret image based information can be decoded by using specific number of share placing one on another. But it has a poor visual quality.

3. THE PROPOSED SCHEME

The natural-image-based visual secret sharing scheme can share a digital secret image over n-1 arbitrary natural images (natural shares) and one share. Instead of changing the contents of the natural shares, here features from each natural share are extracted. These unaltered natural shares are not harmful, thus reducing the interception probability of these shares. The calculated share that is noise-like can be identified by using data hiding techniques to increase the security level during the transmission phase. The natural image- based visual secret sharing scheme uses diverse media as a carrier hence it has many possible scenarios for sharing secret images.
Instead of generating a secret random key, we extract the secret key from an arbitrarily picked natural image in the (2, 2) natural-image-based visual secret sharing scheme. The natural image and the generated share i.e., cipher text were distributed to two users. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the original secret image.

In the natural-image-based visual secret sharing scheme, the natural shares can be gray or color photographs of scenery, hand-painted pictures, family activities, web images, flysheets, photographs, or bookmarks. The natural shares can be in or printed or in digital form. The encryption or encoding process only taken out the features from the natural shares it does not change the natural shares.

4. METHEDOLOGY

The common picture based visual secret sharing plan can share an advanced secret picture over n-1 discretionary common pictures (normal shares) and one offer. As opposed to changing the substance of the common shares, here elements from every characteristic offer are separated. These unaltered common shares are not destructive, along these lines lessening the block attempt likelihood of these shares. The computed offer that is clamor like can be distinguished by utilizing information covering up methods to expand the security level amid the transmission stage. The natural image- based visual secret sharing plan utilizes differing media as a bearer subsequently it has numerous conceivable situations for sharing secret pictures.
The proposed method includes two main phases as shown by the flow diagram below:
1) Efficient design of Cover image.
2) Decryption of Secret images.

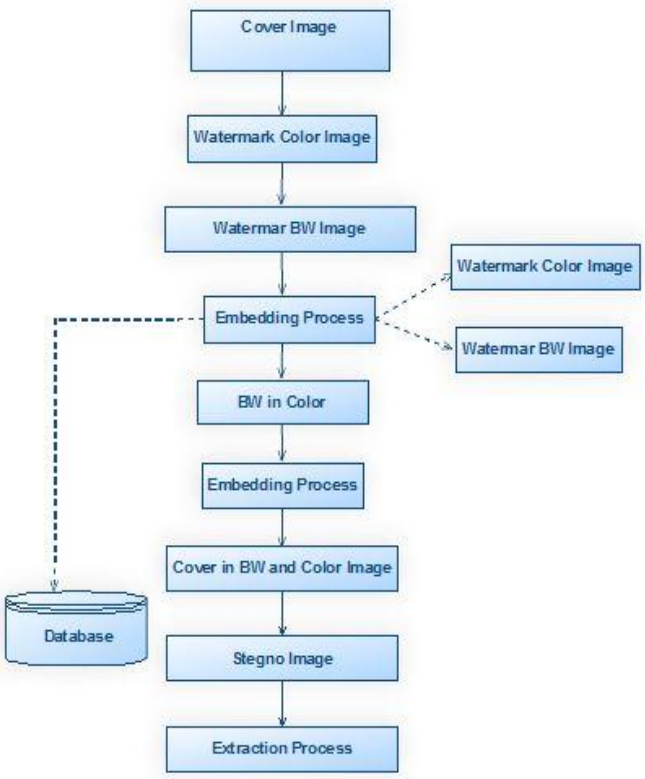

Fig -1: Block Diagram

The proposed (n, n) Natural-picture based visual secret sharing plan can encipher a genuine nature secret picture by n-1 harmless regular shares and one noise like or trivial offer. For first picture, we show a bit with the same weighted esteem in the same shading as somewhat plane; then a real nature secret picture has 24 bit-planes. Accordingly, the element pictures and the noise like offer likewise are reached out to 24 bit-planes. All bit-plane of a component picture contains a double element framework that compares to the same bit-plane as the secret picture.

During Encryption of secret images embedding process is done by two times and efficient design of digital image is done as follows:

First select a basic cover image from image database in this selected cover image we are going to embedded other secret images. After selection of cover image we do resize of cover image just for our convenience and saved this resized cover image. Then we are going to select secret images in this secret image one of the image is color image and other one is bitwise black and white image. Before doing embedding of secret image in cover image we would like to do embedding of bitwise image into color image, to do that we resize the bitwise image into the size which is lesser than color image and selected color image is also resized into size to get fitted into cover image. The resized bitwise image is converted into column image this column version of bitwise image in embedded into pixel of resized color image. Now each pixel of color image has information about bitwise black and white image after that save the embedded version of color image. Again convert the embedded color image into column image now we are doing second stage of embedding process. The column version of embedded color image is taken pixel by pixel and placed in each pixel of cover image. After completion of two stage of embedding process we have cover image contain two secret image embedding on it. During decryption first select the embedded cover image as an input we first extract the color image information form cover image then from decoded color image we extract the information about bitwise black and white image.

5. EXPERIMENTAL RESULTS

To exhibit achievability of the proposed technique several times proposed technique is applied on different images. The following figure shows the simulation results.

Fig -2: Cover Image

Fig -3: Color Image

Fig -4: Bitwise Image

Fig -5: Embedded Color image

Fig -4: Embedded cover image

6. CONCLUSION

The Visual secret sharing scheme that can share a computerized picture utilizing assorted picture media. The media that include numerous arbitrarily picked images are unaltered in the encryption stage. Subsequently, they are absolutely harmless. Despite the quantity of member's expansions, existing VSS Scheme employs only one noise share for exchanging the secret image. The proposed technique effectively minimizes transmission risk and provides friendliness to user for both shares and participants.

REFERENCES

[1]] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, "Incrementing visual cryptography using random grids," Opt. Commun., vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[4]] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

[5]] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," Int. J. Pattern Recognit. Artif. Intell. vol. 21, no. 5, pp. 879–898, Aug. 2007.

[7] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[8] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[10] I. Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.

[11] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[12] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," Digit. Signal Process. vol. 20, no. 6, pp. 1758–1770, Dec. 2010.

[13] Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," Pattern Recognit. Lett. vol. 33, no. 12, pp. 1594–1600, Sep. 2012.

