A Cryptography technique for Data Embedding in Pixel

Banupriya M

[1](Electronics and Communication PPG college of Engineering, Coimbatore,India, banupriyamurugesam@gmail.com)

Abstract*—Visual cryptography (VC) is a technique of encoding a important secret image hooked on shares such that loading an adequate number of shares exposes the secret image. Shares are generally offered in transparencies. Each observer holds a transparency. Most of the existing work on VC focuses on cultivating two parameters: pixel expansion and contrast. In this paper, we considered the cheating problem in VC and extended VC. This system considered the attacks of wicked adversaries who may turn from the scheme in any way. This system offered three cheating methods and useful them on attacking existent VC or extended VC schemes.The proposed a common method that alters a VCS to another VCS that has the belongings of cheating prevention. The above of the conversion is close to optimal in both contrast digressions and pixel expansion*

***Keywords*—** *Visual Cryptography, Pixel expansion, contrast Digression, Transparencies, VC Schemes.*

1. INTRODUCTION

Data hiding is a method that covers data into a carrier for conveying secret messages confidentially .Digital images are widely transmitted over the Internet; therefore, they often serve as a importer for secret transmission. Images used for carrying data are termed as cover images and images with data inserted are termed as stegoimages. Later embedding, pixels of cover images will be altered and alteration occurs[1]. The alteration caused by data embedding is called the embedding distortion. A good data-hiding method should be skilled of avoiding visual and statistical detection while providing an adjustable payload. The least significant bit substitution method, referred to as LSB here, is a well- known data-hiding method[3]. This method is stress-free to implement with reduced CPU rate, and has become most popular embedding techniques. Though, in LSB embedding, the pixels with non-odd values will be increased by one or kept original. The pixels with odd values will be decreased by one or kept original. Therefore, the imbalanced embedding alteration arises and is exposed to steganalysis[2] .In 2004,[8] Chan et al. Proposed a simple and efficient optimal pixel adjustment process (OPAP) method to reduce the alteration caused by LSB replacement. In their method, if message bits are embedded into the rightmost LSBs of a -bit pixel, other bits are adjusted by a simple evaluation. Namely, if the adjusted result offers a smaller distortion, these bits are either replaced by the adjusted result or otherwise kept unmodified.

The LSB and OPAP methods apply only one pixel for an embedding unit, and hide information into the right-most LSBs. Some other group of data-hiding techniques applies two pixels as an embedding unit to hide a message digit in a -ary notational system We term these data-hiding techniques as pixel pair matching (PPM)[4]. In 2006,[9] Mielikainen nominated an LSB agreeing technique based on PPM. He applied two pixels for an embedding unit.The LSB of the first pixel is used for conveying one message bit, when a binary function is applied to carry another bit. In Mielikainen's technique, two bits are expressed by two pixels. There is a 3/4 fortune a pixel value has to be altered by one even another 1/4 chance no pixel gets to be altered. Accordingly, the MSE while payload is 1 bpp. In contrast, the MSE received from LSB is 0.5. In the same year, Zhang and Wang [10] proposed an exploiting modification direction (EMD) method. EMD improves Mielikainen's method in which only one pixel in a pixel pair is changed one greyscale unit at the most and a content digit in a 5-ary notational system can be embedded. Hence, the payload is bpp.LSB matching and EMD techniques greatly improve the conventional LSB technique in which a improve stego image quality can be attained under the equivalent pay-load. Yet, the maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively. Therefore, these two techniques are not suited for applications expecting high payload. The embedding technique by LSB matching and EMD provides no mechanism to increment the payload. In 2008, Hong delivered a data-hiding technique based on Sudoku solutions to attain a maximum payload of bpp[4]. In 2009[1], Chao et al. Proposed a diamond encoding (DE) method to enhance the payload of EMD further. DE employs an extraction function to generate diamond characteristic values (DCV), and embedding is done by modifying the pixel pairs in the cover image according to their DCV's neighborhood set and the given message digit. Instead of enhancing the payload of EMD, Wang et al. in 2010[3] proposed a novel section-wise exploring modification direction method to enhance the image quality of EMD[5]. Their method segments the cover image into pixel sections, and each section is partitioned into the selective and descriptive groups. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. This method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than that of the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality of the stego image is enhanced.

Another group of rather practical data hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These methods may either be implemented by avoiding embedding the message into the con-spicuous part of the cover image, or by improving the embedding efficiency, that is, embed more messages per modification into the cover . The former can be achieved, for example, using "the selection channel" such as the wet paper code pro-posed by Fridrich et a[6]l. The latter can be done by encoding the message optimally with the smallest embedding impact using the near-optimal embedding schemes. In these methods, the data bits were not conveyed by individual pixels but by groups of pixels and their positions.

This paper proposes a new technique where the data transformation will take place in a secure way. The Security will be better when compared with the existing one[7]. Here,We use transparencies foils for transforming the data and it is capable of accepting all types of image formats (e.g.: png).The proposed work is much more efficient than the existing.

II. RELATED WORKS

A.OPTIMAL PIXEL ADJUSTMENT PROCESS

OPAP reduces the distortion in the image available in efficient way when compared to LSB(Least Significant Bit). OPAP mainly focus on the image distortion problem in the image. This image distortion problem will result in the LSB replacement. the least significant bit (lsb) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

It is common to allocate each bit a position number, extending from zero to N-1, where N is the number of bits in the binary illustration used. Normally, this is simply the advocate for the matching bit weight in base-2 (such as in 231..20)[6].Although a few CPU manufacturers allocate bit numbers the opposite way (which is not the same as different endianness), the term lsb (of course) remains explicit as an alias for the unit bit.By extension, the least significant bits (plural) are the bits of the amount closest to, and including, the lsb.The least significant bits have the useful property of varying rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By difference, the three most significant bits stay unchanged (000 to 000).Least significant bits are regularly working in pseudorandom number generators, hash functions and checksums.

This method is given as follows,

Let us consider,'v' be the pixel value of an image, Then 'v(r)' be the right most pixel and 'v(l)' be the leftmost pixel. Image segmentation is the process of partitioning a digital image into multiple segments (sets of pixels, also known as superpixels). The goal of segmentation is to shorten and/or change the depiction of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to detect objects and boundaries (lines, curves, etc.) in images[3]. More precisely, image segmentation is the process of assigning a label to every pixel in an image such that pixels with the same label share assured visual characteristics.

The outcome of image segmentation is a set of segments that jointly shield the entire image, or a set of contours mined from the image (see edge detection). Each of the pixels in a region are similar with respect to some characteristic or computed property, such as color, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristic(s). When applied to a stack of images, typical in medical imaging, the resulting contours after image segmentation can be used to create 3D reconstructions with the help of interpolation algorithms like Marching cubes.

B. DIAMOND ENCODING (De)

The basic concept of DE is based on Pixel Pair Matching. It is an extension of EMD method described in section. DE is used to conceal the secret digit in the N-ary notational system into a pixel pair where N = 2k2 +2k + 1 when k ≥ 1, where k is embedding parameter. The Diamond Characteristic value is calculated so that one secret N-ary digit is concealed. Consider, size of the cover image is m*m and secret message digit is a DN, N stands for N-ary notational system. But embedding parameter k should satisfy the following condition:

$[m * m2] \geq |SN|$

Where, |SN| represents no. of secret message digits in the N-ary notational system[4]. Let a, b, x and y be pixel values, the new set of pixel value which is to be found is called neighborhood set denoted by SK (x, y), (a, b) sets of coordinates whose distance (x, y) is less than or equal to k.SK (x, y) = { (a, b) | |a - x| + |b - y| ≤ k } SK| gives us the value of embedded bases with parameter k. Value of |SK| is defined by embedding parameter k, when k=1, 2, 3....N; SK obtained will be|S1|=5, |S2|=13, |S3|=25....and so on respectively.

$|SK| = [((2i + 1)\ ki{=}0) + (2i - 1\ ki{=}1).$

$=1+ [((2i + 1)\ ki{=}1) + (2i - 1\ ki{=}1)].$

$= 1+ [(4i)]\ ki{=}1{=}1{+}k\ k{+}12{*}\ 4{=}\ 1{+}\ 2k\ (k{+}1).$

$= 2k2 + 2k + 1\ (12).$

Now, DCV is calculated for embedding and extracting process by using diamond function f. DCV is calculated as follows

f(x, y) = ((2k + 1) * x + y) mod N

When f (x′, y′) = SB then (x, y) is replaced by under flowing or overflowing, (x′, y′) must be adjusted finely.

Thus, four conditions of adjustments are as follows

1. If $x' > 255$, $x' = x' - N$

2. If $x' < 0$, $x' = x' + N$

3. If $y' > 255$, $y' = y' - N$

4. If $y' < 0$, $y' = y' + N$

In the diamond encoding method, when neighborhood values are found, they form a diamond shape. The payload is given by ½ log2 (2k2 + 2k + 1) bpp. So, it is proved that, pixel vector (x, y) does not go beyond the value embedding parameter k even after embedding is completed. It is concluded that maximum data can be embedded in the cover image[6] without degrading the quality of the stego image.

C. ADAPTIVE PIXEL PAIR MATCHING (APPM)

The common estimate of the PPM-based data-hiding technique is to apply pixel pair as the coordinate, and seeking a coordinate inside a predefined neighborhood set such that the message digit in a N -ary notational system to be hidden.

Data embedding is done along replacing .For a PPM-based technique, say a digit is to be hidden. The range is between 0 and1, and a coordinate has to be found specified. Hence, the range of integers between 0 an1, and each integer essential come at least once. In addition, to contract the distortion, the amount of coordinates in should be as little as possible.[3] The finest PPM technique shall satisfy the following three requirements:

1) There are precise coordinates .

2) The rates of origin function in these coordinates are mutually exclusive.

3) The design should be capable of embedding digits in whatever notational system so that the fine can be decided to attain lower embedding distortion. DE is a data-hiding technique based on PPM. DE greatly raises the payload of EMD although conserving acceptable stego image quality. Even so, there are a lot troubles. First, the payload of DE is decided by the decided notational system, which is controlled by the parametric quantity ; hence, the notational system cannot be randomly picked out. For example, when is 1, 2, and 3, then digits in a 5-ary, 13-ary, and 25-ary notational system are used to embed data, respectively. However, embedding digits in a 4-ary (i.e., 1 bit per pixel) or 16-ary (i.e., 2 bits per pixel) notational system is not supported in DE. Second, where is the extraction function and is in DE is defined by a diamond shape, which may lead to some unnecessary distortion when . In fact, there exists a better other than diamond shape resulting in a smaller embedding distortion. We redefine as well as and then propose a new embedding method based on PPM. This method not only allows concealed digits in any notational system, but also provides the same or even smaller embedding distortion than DE for various payloads.

III. **PROPOSED SYSTEM**

A. VISUAL CRYPTOGRAPHY

Visual Cryptography is the art and science of encrypting the image in such a way that no one apart from the sender and the intended recipient even realizes the original image, security is provided through obscurity. By contrast, cryptography, conceals the unique image, but it does not conceal the fact that it is not the actual image. The Proposed system will be a friendly environment to deal with image. Generally Cryptography riggings support only one kind of image formats but ours will upkeep all types of formats. The proposed system will be established using Swing and Applet technologies; hence it will provide a friendly atmosphere. The implementation of the core for the project, where we implement the visual cryptography, we use LZW Data Compression Algorithm. It is applied for the gray scale images in this method. Proposed a method that allows N-1 planning parties to cheat an honest party in visual cryptography. They take advantage of significant the underlying delivery of the pixels in the shares to create new shares that combine with existing shares to form a new secret message of the tricksters choosing.

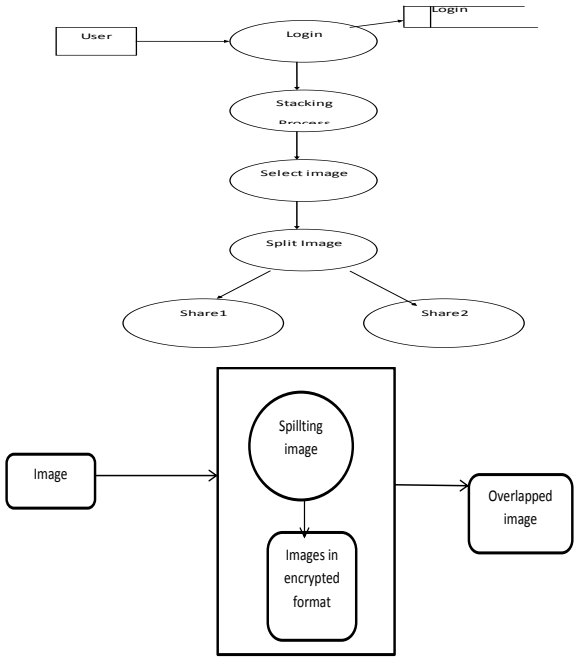
We know that 2 shares are ample to decode the secret image using the human visual system. But inspecting two shares also provide specific information about the 3rd share. For instance colluding participants may examine their shares to determine when they both have black pixels and use that information to [7]regulate that another member will also have a black pixel in that location. Knowing where black pixels exist in another party's share permits them to generate a new share that will combine with the predicted share to form a new secret message. In this way a set of planning parties that have sufficient shares to access the secret code can cheat other truthful parties.

B. AUTHENTICATION

The system would use Login/ Password technique for imposing security at the user level. This would promise authorized access to the private data.The user given login details wil[8]l verify with the database details and allows only the verified users to our system. Other users who don't have correct login details couldn't get into our system to perform stacking and overlapping process.

C. STACKING PROCESS

The visual cryptography is suitable for encryption and distribution of secret information that is available as a black and white pixel image. It splits the information into many transparent foils. That has to be overlayed to retrieve the information. All the split pieces are in unknown format in a specified



D.OVERLAPPING PROCESS

After a Stacking Process, the original image which contains the information will split into several pieces according to the users input. In this module user will locate the folder which contains the pieces of images in encrypted format which is not able to understand by human[10]. Then by using the combination of black and white pixel the images will be overlapped and here the decoding process will take place to decrypt the image back to normal format.

E.RECOVERED PROCESS

Each share was printed on a remove transparency, and decrypting process is performed by overlaying the shares. When all n share was overlaid, the original image would appear. Now human can read the original information present in the received image.

F.ENCODING

The algorithm works by scanning through the input string for successively longer substrings until it finds one that is not in the dictionary[9].The encoding of te data will be done to each and every pixels n he image .The information is splitted into two shares after the splits the encoding is done for all the pixels in the all shares.

G.DECODING

The decoding algorithm works by reading a value from the encoded input and outputting the corresponding string from the initialized dictinary.The final input value is decoded without any more additions to the dictinary.

IV. CONCLUSION

Thus using the concept of visual cryptography which uses various theory of recursive hiding of secrets we are able to prevent the image from cheating from any intruders other than the owner. This provides a method of hiding secrets recursively in the shares of threshold patterns, which provides an efficient utilization of the data[10]. Here we Proposed a construction of EVS which was realized by embedding the random shares into the meaningful covering shares. The shares of the proposed scheme are meaningful images and the stacking of a qualified subset will recover the secret image visually. The visual quality of the share and between the secret image pixel expansion and the visual quality of the shares

REFERENCES

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms,and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 3, no. 3, pp. 32–44,May/Jun. 2003.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.

[4] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in Proc. SPIE, Media Forensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.