Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Visual Cryptography Scheme for Colour Images without Pixel Expansion

K. Vishal[1], P. Sanoop Kumar[2], Sri Sushmitha Akula[3], K Somasekhar[4]

[1, 3] Department of CSE, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, India

[2, 4] Assistant Professor, Department of CSE, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, India

***Abstract*— Visual cryptography is one of such field which provides security for visual data. And the technique proposed through this project provides more than a commendable level of security for visual data. Under this method an image according to the users' specifications is taken as an input and is divided into a set incoherent shares using the proposed decryption algorithm and some protected files. It is more than understood that the essence of this technique revolves around creating and maintaining an air of anonymity around the communication between the sender and the receiver**.

***Keywords* — Visual cryptography, visual data, incoherent shares, decryption algorithm, protected files, sender, receiver.**

I. Introduction

Security is of paramount importance when it comes to any mode of communication. Be it textual form of data or any other, the risk of its interception and pilferage is imminent if a proper security is not provided. And a greater risk is not able to retrieve the information from the encrypted data-"The algorithm becomes a crypt for the information instead of encryption if proper retrieval is jot performed".

II. SYSTEM ANALYSIS

A. Existing System

Visual cryptography (VC), first proposed in 1994 by Naor and Shamir [1], is a secret sharing scheme, based on black and-white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics. For example, biometric information in the form of facial, fingerprint and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined.

A basic 2-out-of-2 or (2; 2) visual cryptography scheme [2] produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k; n) scheme produces n shares, but only requires combining k shares to recover the secret image. To preserve the aspect ratio for the recovered secret image for a (2; 2) scheme each pixel in the original image can be replaced in the share images by a 2 _ 2 block of sub-pixels. If the original pixel is white, one of six combinations of share pixels is randomly created. Similarly, the possible share combination for black pixels is also shown. After stacking the shares with white transparent and black opaque, the original secret image will be revealed. Stacking can be viewed as mathematically ORing, where white is equivalent to "0" and black is equivalent to "1".Note that the resulting share images and the recovered secret image contain 4 times more pixels than the original image (since each pixel of the original image was mapped to four subpixels). It may also be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image

B. Proposed System

The proposed system is an update of the existing system in every way:

- It works with color images also.
- Its output is also a color image.
- Compared to 6 possible permutations for a pixel, this system provides 24 possible permutations.
- There is no pixel expansion as in contrast to existing system.

Through this project, an algorithm is put forth to provide a higher level of security for colour images which was not provided before this. The algorithm proposed takes into account the basic components of a pixel to provide security.

It is known that pixel is the smallest most unit of an image. Every image is made up of thousands of such pixels. Every pixel consists of four important components, namely- alpha (Transparency Factor), red (intensity of red shade), green (intensity of green shade) and blue (intensity of blue shade). The concept of permutations and combinations plays a pivotal role in this algorithm. As it is known a set of dissimilar entities can be arranged in n! (Red as n factorial) ways. In a similar way the four contents of a pixel can be shuffled and arranged in 24 distinct ways.

The algorithm uses this feature to separate pixel contents and distribute them among four different shares at random .A note of the permutation used for each pixel is made in a proper data structure. This algorithm is taken a step further by providing not one, but two ways of encrypting the permutation file. The two ways are **"0-encryption"** and **"1-encryption".**

1) "0-Encryption":

Since array is the most convenient way to represent data, it has been used here to do so. Under this scheme every element whose location co-ordinates add up to an even number is reversed and the ones whose corresponding sum is odd are left untouched. In case single digit numbers are encountered in the former case, they are multiplied by 10. And when these files are decrypted the same logic is used, barring the multiples of 10(10, 20, 30, 40.....) which are divided by 10 get back the original permutation file.

2) "1-Encryption":

It is similar to 0-encryption, the only difference is that if an element's array co-ordinates sum up to an odd number it is reversed and it is left untouched otherwise. And the logic pertaining to encryption of single digit numbers remains same as specified in the earlier scheme. Simply put the two encryption mechanisms are a mirror image of each other, with each having an equal probability of occurrence. And similarly the decryption in this scheme is conducted in accordance as given above.

3) Decryption:

- The encrypted permutation file is used to decrypt the shares and reconstruct the image.
- Since the scheme used for encryption is a symmetric one, the same can be used for decryption too.
- On decryption, we obtain the original permutation file.

4) Reconstructing The Image:

- Similar to the breakdown of the image, reconstruction also involves a set of 24 permutations.
- Each permutation is allotted a number between 1 and 24.
- Every time a number is extracted from the permutation file a corresponding order in which the individual components have to be read from the four shares is established. For example, permutation 2 implies the values from the shares have to be read in the order share1, share2, share4 and share3 in order for the correct pixel to be formed.

5) Efficiency:

Since there are 24 permutations for each pixel, and only one permutation is used, it becomes difficult to find out the correct combination by using brute force approach. The probability of success is 1/24 which leaves us with 23/24 probability of failure i.e., if the actual permutation is not known there is a 95.83% chance of failing in reconstructing a single pixel. Note that this rate of failure increases with each additional pixel. This adds up to an even bigger failure rate given the fact that even a small image on an average has around 10000 pixels.

C. Figures

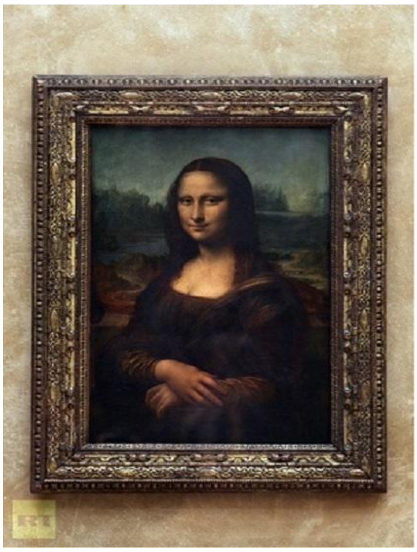


Fig. 1 Original Image

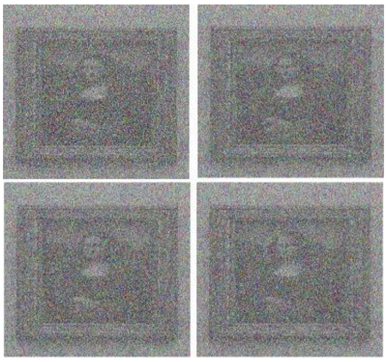


Fig. 2 Intermediate Shares

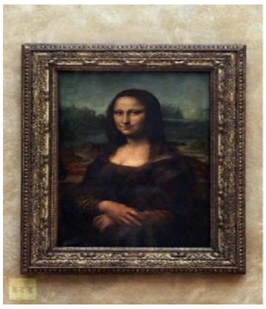
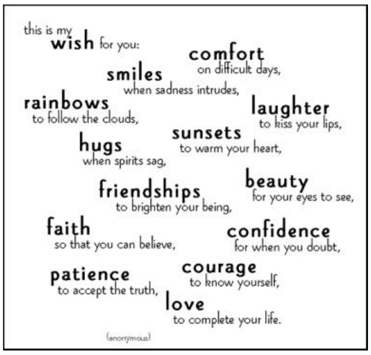


Fig. 3 Reconstructed Image



this is my
wish for you:
comfort
on difficult days,
smiles
when sadness intrudes,
rainbows
to follow the clouds,
laughter
to kiss your lips,
sunsets
to warm your heart,
hugs
when spirits sag,
beauty
for your eyes to see,
friendships
to brighten your being,
faith
so that you can believe,
confidence
for when you doubt,
courage
to know yourself,
patience
to accept the truth,
love
to complete your life.
(anonymous)

Fig. 4 Original Image

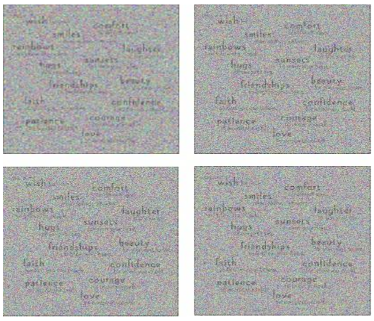
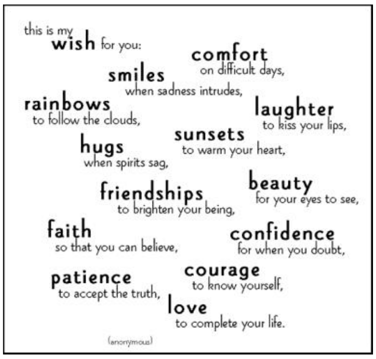


Fig. 5 Intermediate Shares



this is my
wish for you:
comfort
on difficult days,
smiles
when sadness intrudes,
rainbows
to follow the clouds,
laughter
to kiss your lips,
sunsets
to warm your heart,
hugs
when spirits sag,
beauty
for your eyes to see,
friendships
to brighten your being,
faith
so that you can believe,
confidence
for when you doubt,
courage
to know yourself,
patience
to accept the truth,
love
to complete your life.
(anonymous)

Fig. 6 Reconstructed Image

III. Conclusion

In the real time implementation of visual cryptography, realization of color image encryption has not been up to the mark unlike half tone images. This drawback has been more than consolidated through this proposed project both in terms of security and feasibility. And given uniqueness of this project which creates a set of decoy shares which throw the intruder onto the alternative path. And by the time the intruder realizes the mistake the message would have already been conveyed to the sender. Further improvements are on course to create a better level of security, adding to the already strong protection level.

References

[1] M. Naor and A. Shamir, “Visual cryptography”, in EUROCRYPT’94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995

[2] N. Askari, H.M. Heys, and C.R. Moloney, “An Extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images” IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) E vol. 6, no. 1, pp 33-38, 2013