ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Layered Morphing With Image Cryptography

[1]Vijaya Pinjarkar, [2]Vivek Singh, [3]Aditya Thakker, [4]Parita Todai

[1]Assistant Professor, Department of Information Technology, K.J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai, Maharashtra, India

[2,3,4]Bachelor of Information Technology, Department of Information Technology, K.J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai, Maharashtra, India

.

ABSTRACT: Morphing of images has evolved and become a challenging field in information hiding and data security.The primary objective is providing protection of highly sensitive data using the concept of cryptography as well as Layered Morphing. Layered Morphing is a secret-sharing technique that divides the encrypted secret image into several shares. In this system we have proposed a new technique to enhance the security in visual cryptography. The user will be provided with a system which will help protect the confidential information with the help of Layered Morphing. Initially the original image will be provided by the user; this image will be used to provide security to the data. To upload an image, a password has to be set. The image is then divided into 4 layers and stored at different locations. Whenever user wants to access his confidential data he has to merge these 4 layers from different locations in proper order to form the original image .But layers of images that are formed are morphed images, so it is almost impossible for the user to identify the original image just by looking at the shares of morphed images. In order to add further security, after retrieving the original image the same password will be asked by the system and only after entering the right password , user can access the confidential data.

KEYWORDS: VisualCryptography, Image Morphing, Pixels, Layered Morphing.

I. INTRODUCTION

In the present era, the data transfers using internet is rapidly increasing because it is convenient as well as fast to transfer the data to destination. But sharing of such data without storing it, becomes tedious job to retain for further use. Here security is an important concern. Since many of the individuals and business people use to transfer organizational documents, supreme information using internet, it is necessary to maintain the confidentiality. There is a risk of any unauthorized individual hacking the data if he knows the location.

Visual Cryptography is a crypto logical technique that permits visual data (pictures, text, etc.) to be encrypted in such some way that coding becomes a mechanical operation that doesn't need a pc or hard-coreprogramming [2]. one among the known techniques has been attributable to Moni Naor and Adi Shamir, World Health Organization developed it in 1994[9].They expressed a visible secret sharing theme, wherever a picture was variable into n shares so solely somebody with all n shares might decode the image, whereas any n − one shares discovered no data regarding the first image. every share was written on a separate transparency, and coding was performed by overlaying the shares. Once all n shares were overlaid, the first image would seem[10].

Morphing is a notable technique in the field of motion pictures and animations that changes smoothly from one image or shape into another through a seamless transition. Layered Morphing is a secret-sharing method that encrypts a secret image into several shares. Simply by combining the component shares the secret image becomes clearly visible.

II. RELATED WORK

Based on report and investigation on existing system, this system has additional feature than previous one.Previously the recovered image had a degraded quality as the compression ratio was large. This led to a decreased contrast between the white and black pixels. The existing system does not provide a friendly environment to encrypt or decrypt

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

the data.The system supports only one kind of format. A basic a pair of-out- of-2 or (2; 2) visualcryptographythemeproduces 2 share pictures from a resourceful image and should stack each shares to breed the initial image. Typically, a (k; n) theme produces n shares, however solely needs combining k shares to recover the key image. [9]

To preserve the ratio for the recovered secret image for a (a pair) theme every element within the original image will be replaced within the share pictures by a pair of X 2 block of subpixels. If the initial element is white, one in all six combos of share pixels is randomly created. Once stacking the shares with white clear and black opaque, the initial secret image are discovered. Stacking will be viewed as mathematically ORing, wherever white depicts "0" and black depicts "1". Note that the ensuing share pictures and also the recovered secret image contain four times additional elements than the initial image (since every pixel of the initial image was mapped to four subpixels). Note that the recovered image includes degradation in visual since a recovered white element has 4 subpixels (2 black, 2 white) whereas a black element also has 4 subpixels(All black).

III. PROPOSED ALGORITHM

We propose a system for processing colour images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme called Layered Morphing for which the format will be jpeg and png. The resulting scheme maintains the perfect security of the original with extended visual cryptography approach of Layered Morphing .The proposed system can support more than one type of format .The proposed system uses XOR algorithm to protect the data . We are also going to use a password to further protect the data .Using a key along with XOR will make the resulting encryption scheme provably unbreakable.

The image will be split into two component images. for every pixel in the original image there exist a pair of component image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one {black, white}, and the other {white, black}. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match: both {black, white} or both {white, black}. When these matching pairs are overlapped, they will appear light gray.

So, when the two component images are imposed on each other, the original image reappears. However, the component images themselves does not reveal any information about the original image.
There is a simple algorithm for Visual cryptography with Layered Morphing that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows: First create an image of random pixels the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color.

If a pixel of the original image is different than the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the same color as the corresponding pixel of the first encrypted image. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

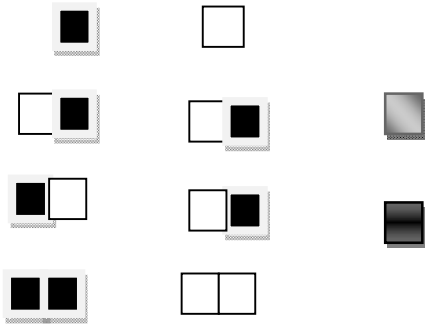
Encoding of pixels:

Original Pixel

Layer1

Layer2

Overlaid



IV. ARCHITECTURE OF PROPOSED SYSTEM

The architecture of the complete system consist of two parts: 1.) Encryption 2.) Decryption

Encryption:

The encryption part consists of the usage of a original image by the legitimate user to protect the sensitive data. The user uploads a coloured image which he wants to use to secure the information. The image uploaded by the user is either in .jpeg or .png format. The main aim of the encryption part is to divide the image in to layers so that it becomes difficult for the unauthorised user to identify the image using those parts. The image uploaded by the user gets divided in to 4 parts using the X-OR technique. The image is thus morphed and forms part.

The parts thus formed does not visually denote the original image and it becomes impossible for any user to identify the original image by the formed layers .The layers thus formed are stored in to different locations so that it becomes difficult for the user to trace the parts required to form the original image.

Decryption :

The encryption part thus states that the authenticated user has set used an image to protect the data along with the concept of layered morphing . The new user will have to decrypt this technique sued by the original user to protect the data .The user will now have to provide the location of all the parts that are set by the original user . The new user who is not aurthorised will not be able to determine the location of the layers by just looking at the images . The new user will arrange all the parts and thus the original image will be retrieved . The user will also have to enter the password set by the original authenticated user in order to access the data .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

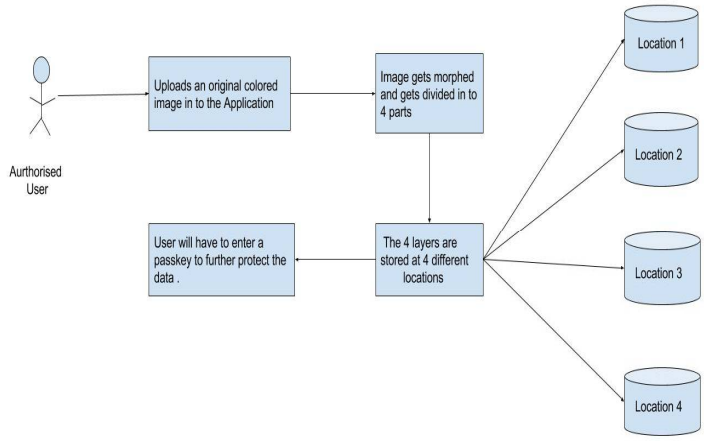


Fig6: Encryptionand Storing

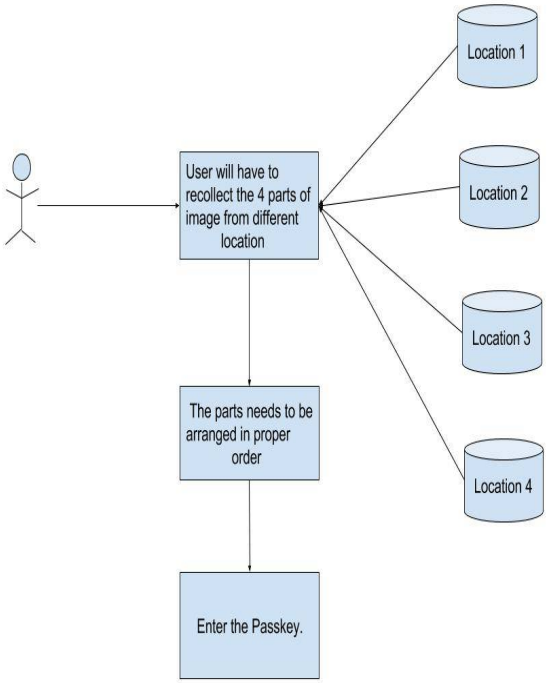


Fig7: Decryption and Retrieval

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

V. SIMULATION AND RESULTS

COMPARISON OF EXISTING SYSTEM AND PROPOSED SYSTEM

Existing system	Proposed system
Each pixel of original image has 4 pixels of the mapped image, 2 white and 2 black subpixels for 1 original white pixel , and 4 black subpixels for original black pixel	Each component image has a pair of pixels for every pixel in the original image.
White gets transparent (0 of binary), and black gets opaque (1 of binary)	Original black gets dark grey as the component images must be complementary,while Original white gets light grey , as the component images should match.
Recovered image is degraded as it is 4 times the original image	Recovered image is much better in quality as the local ratio of pixels of color images is much close to the ratio of original image.
Security is weak , since the original image has a poor contrast of black and white	Maintains perfect security by providing extra security of entering

VI. CONCLUSION AND FUTURE WORK

The proposed system aims to simplify the complex and tedious process with the flexible and simple process. The proposed system is being developed as an attempt to overcome the difficulties of the existing system. The following are the highlights of the proposed system

1) It provides two levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways.

2) This application can be used to increase the security on highly sensitive data. The user will be asked to provide the password even if he finds the location of images and is able to decrypt it. It can be used as advancement over the existing option to input the security phrase.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

3) In the case of a secret file being encrypted the morphed layers can be kept inside a local directory or dive .This secret file can be stored in the normal way. In case of layered streams part of image can be sent in each location. This will increase the security of the system, however the time consumption will increase in this case.

ACKNOWLEDGEMENTS

We wish to express our sincere gratitude to Prof. Mrs. Vijaya Pinjarkar, Project Guide for providing us an opportunity to do our project work in security domain. We sincerely thank Mr. Uday Rote, HOD of IT Department and Mr. Harsh Bhor, Project Coordinator for their guidance and encouragement in carrying out this project work. We also wish to express our gratitude to the officials and other staff members of K.J Somaiya Institute of Engineering and Information Technology, who rendered their help during the period of our project work.

REFERENCES

[1] G. Wolberg, Recent advances in image morphing, EProc. Computer Graphics International (CGIE6), pp. 64-71, 1996.
[2] M. Steyvers, Morphing techniques for manipulating face images, Behavior Research Methods, Instruments, and Computers, Vol. 31, No.2, pp. 359-369, 1999.
[3] S. Kondo and Q. F. Zhao, "A novel steganographic technique based on image morphing," Proc. International Conference on Ubiquitous Intelligence and Computing (UIC06), Wuhan and Three Gorges, China, pp. 806-815, Sept. 2006 (Lecture Notes in Computer Science 4159, Springer).
[4] S. Katzenbeisser and F. A. P. Peticolas, Information hiding: techniques for steganography and digital watermarking, Artech House, 2000
[5] T. Lewellen, "BREACH vulnerability in compressed HTTPS", http://www.kb.cert.org/vuls/id/987798, Vulnerability Notes Database,2013.
[6] Visual Cryptography and Secret Image Sharing by Stelvio Cimato, Ching-Nung Yang
[7]Visual Cryptography and its Applications by J.P. Weir,Weiqi Yan.
[8]Investigators guide to stegnography by Gregory Kipper .
[9] M. Naor and A. Shamir, "Visual Cryptography" in EUROCRYPT '94,Berlin,1995,Vol LNCS 950,pp 1-12,Springer-Verlag.
[10] Verheul, E.R. and H.C.A.van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography, 11(2):179–196, 1997.
[11] Ryota Hanyu and Kazuki Murakami ,Verification of an image morphing based technology for improving the security in cloud storage services ,978-1-4799-4476-7.