Information Science and Technology
ISSN: 0976-917X & ISSN: 0976-9188, Volume 3, Issue 2, 2014, pp.-060-065.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BIJ0000002

IMPROVED VISUAL CRYPTOGRAPHY SCHEME FOR DATA SECURITY

KESHAMONI K.* AND HARIKRISHNA M.
Department of ECE, RVR Institute of Engineering & Technology, JNTU, Hyderabad- 500 085, AP, India.
*Corresponding Author: Email- kumar.keshamoni@gmail.com

Received: November 08, 2013; Accepted: July 10, 2014

Abstract- Cryptography is that the observe and study of concealment info. Cryptography, then, not solely protects knowledge from larceny or alteration, however can even be used for user authentication. There are, in general, 3 styles of scientific discipline schemes usually won't to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. Altogether cases, the initial unencrypted knowledge are said as plaintext. It's encrypted into cipher text, which can successively (usually) be decrypted into usable plaintext. Visual Cryptography could be a kind of cryptography that encodes variety of pictures within the approach that once the pictures on transparencies square measure stacked along, the hidden message seems while not a trace of original pictures. The decipherment is completed directly by the human sensory system with no special scientific discipline calculations. This project presents a system that takes 3 photos as Associate in nursing input and generates 2 pictures that correspond to 2 of the 3 input photos. The third image is reconstructed by printing the 2 output pictures onto transparencies and stacking them along. Whereas the previous researches essentially handle solely binary pictures, this project establishes the extended visual cryptography theme appropriate for natural pictures. Generally, visual cryptography suffers from the deterioration of the image quality. This project additionally describes the strategy to boost the standard of the output pictures. The trade-off between the image quality and therefore the security square measure mentioned and assessed by perceptive the particular results of this methodology. Moreover, the improvement of the image quality is mentioned.

Keywords- Cryptography, Pixel, MATLAB, encrypted, VSSS, watermarking, threshold, Decryption, Steganography

Citation: Keshamoni K. and Harikrishna M. (2014) Improved Visual Cryptography Scheme for Data Security, Information Science and Technology, ISSN: 0976-917X & ISSN: 0976-9188, Volume 3, Issue 2, pp.-060-065.

Introduction

Image

A digital image could be a data file that contains graphical data rather than text or a program. Pixels square measure the fundamental building blocks of all digital pictures. Pixels square measure little abutting squares during a matrix across the length and dimension of your digital image. They're thus little that you simply don't see the particular pixels once the image is on your pc monitor. Pixels square measure monochromatic. Every component could be a single solid color that's mixed from some combination of the three primary colours of Red, Green, and Blue. So, each component features a RED element, a inexperienced element and BLUE element.

The physical dimensions of a digital image area unit measured in components and usually known as pixel or image resolution. Pixels area unit scalable to completely different physical sizes on your laptop monitor or on a photograph print. However, all of the pixels in any explicit digital image area unit an equivalent size. Pixels as described in an exceedingly written photograph become spherical slightly overlapping dots. As shown during this bitonal image, every component is allotted a tonal price, during this example zero for black and one for white. Component dimensions area unit the horizontal and vertical measurements of a picture expressed in pixels. The component dimension is also determined by multiplying each the dimension and therefore the height by the dpi. A photographic camera will have component dimensions, expressed because the range of pixels horizontally and vertically that outline its resolution (e.g., 2,048 by 3,072). Calculate the dpi achieved by dividing a document's dimension into the corresponding component dimension against that it's aligned.

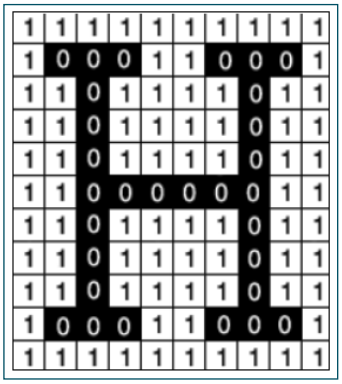

Fig. 1- Pixel Representation

Images in MATLAB

The basic structure in MATLAB is that the array, associate ordered set of real or complicated components. This object is of course suited to the illustration of pictures, real-valued ordered sets of color or intensity knowledge. MATLAB stores most pictures as two-dimensional arrays (i.e., matrices), within which every component of the matrix corresponds to one picture element within the displayed image.

Image Representation

An image is keep as a matrix victimization normal Matlab matrix convention. There area unit four basic kinds of pictures supported by Matlab:

1. Binary pictures
2. Intensity pictures
3. RGB images
4. Indexed pictures

Visual Cryptography

Introduction to Visual Cryptography

Visual cryptography may be a cryptographical technique that permits visual info (pictures, text, etc.) to be encrypted in such the way that the cryptography will be performed by the human sensory system, while not the help of computers. Visual cryptography was pioneered by Moni and Shamir [8]. They demonstrated a visible secret sharing theme, wherever a picture was shifting into n shares so solely somebody with all n shares might rewrite the image, whereas any n-1 shares disclosed no info regarding the initial image. Every share was written on a separate transparency, and cryptography was performed by overlaying the shares. Once all n shares were overlaid, the initial image would seem. Employing a similar plan, transparencies will be accustomed implement a one-time pad cryptography, wherever one transparency may be a shared random pad, and another transparency acts because the cipher text. Visual cryptography may be a quite cryptography that may be decoded directly by the human sensory system with none special calculation for cryptography. As shown in below figure, our visual cryptography system takes 3 footage as AN input and generates 2 pictures that correspond to 2 of the 3 input footage. The third image is reconstructed by printing the 2 output pictures onto transparencies and stacking them along. This sort of visual cryptography, that reconstructs the image by stacking some meaningful pictures along, is very referred to as Extended Visual Cryptography. During this project, the images shown on the output images area unit referred to as sheets and therefore the ensuing image reconstructed by stacking the 2 sheets along is termed the target. Previous works on the extended visual cryptography contend with binary pictures like text pictures, however natural pictures like pictures area unit troublesome to handle in such theme.

This paper establishes the extended visual cryptography theme for natural pictures. Generally, visual cryptography suffers from the deterioration of the image quality. This project additionally describes the strategy to boost the standard of the output image. There area unit several powerful secret-sharing schemes that modify you to inscribe a document or file so no one will decipher the $64000 contents of the encoded document while not access to the encrypted shares and a pc to perform the calculations necessary to rewrite the key document. Visual Cryptography may be a secret-sharing technique that encrypts a secret image into many shares however needs neither pc nor calculations to rewrite the key image. Instead, the key image is reconstructed visually: just by overlaying the encrypted shares the key image becomes clearly visible. Visual Cryptography may be a special cryptography technique to cover info in pictures in such the way that it will be decrypted by the human vision if the proper key image is employed. Visual Cryptography uses 2 clear pictures. They demonstrated a visible secret sharing theme, wherever a picture was shifting into n shares so solely somebody with all n shares might rewrite the image, whereas any n-1 shares disclosed no info regarding the initial image. Every share was written on a separate transparency, and cryptography was performed by overlaying the shares. Once all n shares were overlaid, the initial image would seem. One image contains random pixels and therefore the alternative image contains the key info. It's not possible to retrieve the key info from one in all the photographs. Each clear pictures and layers area unit needed to reveal the knowledge.

The easiest thanks to implement Visual Cryptography is to print the 2 layers onto a clear sheet. Once the random image contains really random pixels it will be seen as a One-time Pad system and can supply unbreakable cryptography. Within the overlay animation you'll be able to observe the 2 layers slippery over one another till they're properly aligned and therefore the hidden info seems. Visual cryptography may be a cryptographical technique that permits visual info (pictures, text, etc.) to be encrypted in such the way that the cryptography will be performed by the human sensory system, while not the help of computers. Visual cryptography may be a common answer for image cryptography. Mistreatment secret sharing ideas, the cryptography procedure encrypts a secret image into the questionable shares that area unit noise-like secure pictures which might be transmitted or distributed over AN unreliable communication. mistreatment the properties of the human sensory system to force the popularity of a secret message from overlapping shares, the key image is decrypted while not further computations and any data of cryptography. Visual cryptographical solutions treat binary or binarized inputs. Therefore, natural (continuous-tone) pictures should be 1st born-again into halftone pictures by mistreatment the density of internet dots to simulate the initial grey or color levels within the target binary illustration. Then, the halftone version of the input image is employed rather than the initial secret image to supply the shares. The decrypted image is obtained by stacking the shares along. as a result of binary information will be displayed either as opaque or clear once written on transparencies or viewed on the screen, overlapping shares that contain apparently random info will reveal the key image while not further computations or any data of cryptographical keys. However, thanks to the character of the algorithmic program, the decrypted image is darker, contains variety of visual impairments, and most of visual cryptography solutions increase the special resolution of the key image. Additionally, the necessity for inputs of the binary or dithered nature solely limits the relevancy of visual cryptography. Most of the prevailing secret sharing schemes area unit generalized among the questionable-thres hold framework that confidentially divides the content of a secret message into n shares within the manner that needs the presence of a minimum of k, for k≤n, shares for the key message reconstruction, Thus, the framework will use any of n!/(k!(n−k)!) potential mixtures of k shares to recover the key message, whereas the employment of k−1 or less shares mustn't reveal the key message.

Construction Algorithm for a (2, 2) - Threshold Scheme

- Construct two 2*x*2 basis matrices as:

$$S0 = \begin{bmatrix} 10 \\ \\ 10 \end{bmatrix}$$

$$S1 = \begin{bmatrix} 10 \\ \\ 10 \end{bmatrix}$$

- Exploitation the permutated basis matrices, every element from the key image are going to be encoded into 2 sub pixels on every participant's share. A black element on the key image are going to be encoded on the ith participant's share because the ith row of matrix S1, wherever a one represents a Black sub element and a '0' represent's a white sub element. Similarly, a white element on the key image is going to be encoded on the ith participant's share because the ith row of matrix S0.
- Before secret writing every element from the key image onto every share, indiscriminately turn the columns of the premise matrices S0 and S1.
- This VCS (Visual Cryptography Scheme) divides every element within the secret image into m=2 sub pixels.
- It's a distinction of α(m)•m=1 and a relative distinction of α(m) =1/2.

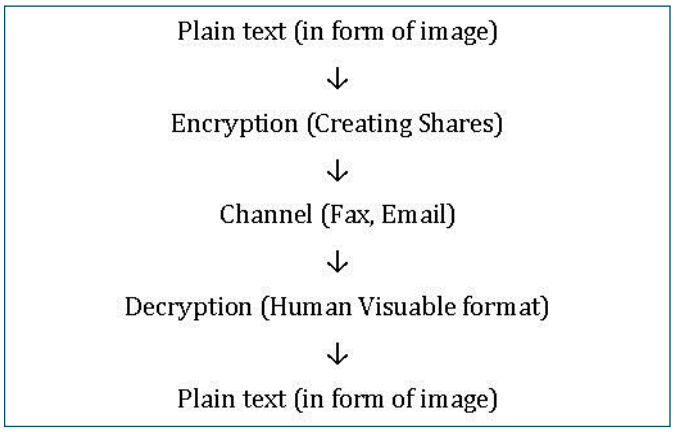

Fig. 2- Block Diagram of Visual Cryptography

Working of Visual Cryptography

Initially the unencrypted knowledge that's mentioned as Plain text is initial encrypted that's transferring the plain text into code format that is non legible format. Then the code is gone through the channel i.e. Fax or email then coding is finished that's the encrypted knowledge that is within the non legible format is born-again into human legible format. Thus the initial knowledge the plain text is obtained. Within the means image the image or the text is encrypted and decrypted. Once more the first image or text is obtained once the coding. Each picture element of the pictures is split into smaller blocks. There square measure forever identical variety white (transparent) and black blocks. If a picture element is split into 2 elements, there square measure one white and one black block. If the picture element is split into four equal elements, there square measure 2 white and 2 black blocks. The instance pictures from higher than uses pixels that square measure divided into four elements. If a pixel, divided into four elements, will have six completely different states. If a picture element on layer one includes a given state, the picture element on layer two could have one in every of 2 states: identical or inverted to the picture element of layer one. If the picture element of layer two is a twin of layer one, the overlayed picture element are going to be [*fr1] black and [*fr1] white. Such overlayed picture element is named gray or empty. If the pixels of layer one and a pair of square measure inverted or opposite, the overlayed version are going to be fully black. This is often Associate in Nursing data picture element. We will currently produce the 2 layers. One clear image, layer 1, has pixels that all have a random state, one in every of the six potential states. Layer two is a twin of layer one, aside from the pixels that ought to be black (contain information) once overlayed. These picture elements have a state that's opposite to identical pixel in layer1. If each pictures square measure overlayed, the areas with identical states can look grey, and therefore the areas with opposite states are going to be black. The system of picture element will be applied in numerous ways in which. In our example, every picture element is split into four blocks. However, you'll be able to conjointly use pixels, divided into 2 parallelogram blocks, or maybe divided circles. Also, it does not matter if the picture element is split horizontally or vertically. There square measure many alternative picture element systems, some with higher distinction, higher resolution or maybe with color pixels. If the picture element states of layer one square measure really (crypto secure) random, each empty and data pixels of layer two also will have fully random states. One cannot grasp if a picture element in layer two is employed to make a gray or black picture element, since we want the state of that picture element in layer one (which is random) to grasp the overlay result. If all needs for true randomness square measure consummated, Visual Cryptography offers absolute secrecy consistent with the data Theory. If Visual Cryptography is employed for secure communications, the sender can distribute one or a lot of random layers one earlier to the receiver. If the sender includes a message, he creates a layer two for a selected distributed layer one and sends it to the receiver. The receiver aligns the 2 layers and therefore the secret data is discovered, this whiles not the necessity for Associate in Nursing encoding device, a laptop or activity calculations by hand. The system is unbreakable, as long because the 2 layers do not fall along within the wrong hands. once one in every of each layers is intercepted it's not possible to retrieve the encrypted data.

Encryption

In cryptography, secret writing is that the method of remodeling data (referred to as plaintext) exploitation associate algorithmic program (called a cipher) to form it undecipherable to anyone except those possessing special information, sometimes said as a key. The result of the method is encrypted data (in cryptography, said as cipher text). The reverse method, i.e., to form the encrypted data clear once more, is said as decipherment (i.e., to form it unencrypted). In several contexts, the word secret writing may implicitly discuss with the reverse method, decipherment e.g. "software for encryption" will generally additionally perform decipherment. Secret writing has long been utilized by militaries and governments to facilitate secret communication. It's currently ordinarily employed in protective data among several types of civilian systems. for instance, the pc Security Institute according that in 2007, seventy one of firms surveyed used secret writing for a few of their information in transit, and fifty three used secret writing for a few of their information in storage secret writing is wont to defend information "at rest", like files on computers and storage devices (e.g. USB flash drives). In recent years there are varied reports of confidential information like customers' personal records being exposed through loss or stealing of laptops or backup drives. Encrypting such files at rest

helps defend them ought to physical security measures fail. Digital rights management systems that forestall unauthorized use or replica of proprietary material and defend code against reverse engineering (see additionally copy defendion) square measure another somewhat completely different example of exploitation secret writing on information at rest secret writing is additionally wont to protect information in transit, for instance telephones, wireless microphones, wireless intercommunication system systems, Bluetooth devices and bank cash machine machines. There are varied reports {of information|of knowledge|of information} in transit being intercepted in recent years Encrypting data in transit additionally helps to secure it because it is commonly tough to physically secure all access to network.

Encoding Process

Choose data to be encrypted, say Mi. victimisation the said algorithmic program of visual cryptography, divide the content of the message (Mi) into n shares (here we tend to get initial level of concealing. every share are treated as data. Shares is treated as one image or totally different. If shares are treating as one image we are able to hide it along within one Image. Else we want {different|totally totally different|completely different} pictures to different shares. Choose associate degree applicable image or pictures in order that the share of the initial message is embedded in to one image or every share in numerous pictures. Rather than causation the n shares straightaway it'll be embedded in to an image or pictures victimisation any of the steganography technique. (Here we tend to get second level of hiding). If we are using different images to store different shares it will be much secure and very difficult to find out the information by the intruders. But need different Images. Use DCT-Steg encryption method to code the shares (which includes the key knowledge).

Decryption

Decryption is that the reverse operation of secret writing. For secret -key secret writing, you want to understand each the key and IV that was won't to code the information. For public-key secret writing, you want to understand either the general public key (if the information was encrypted victimisation the personal key) or the personal key. The decryption of data encrypted with symmetric algorithms is similar to the process used to encrypt data with symmetric algorithms. The Crypto Stream category is employed with bilaterally symmetric cryptography categories provided by the .NET Framework to decode information scan from any managed stream object.

Decoding Process

- Use DCT- Steg cryptography method to rewrite the shares from pictures.
- Once cryptography the message from the quilt medium [Here image/images] we'll get the n shares of the message. they're in encrypted type. That's encrypted by visual cryptography.
- These n shares will then be decrypted by human sensory system, while not the aid of computers. We want no computing mechanism to rewrite the message encrypted by visual cryptography. What we tend to solely want is to super impose all the n shares on each other so we'll get the initial message.

Differences between Cryptography and Steganography

Cryptography and steganography ar accepted and wide used techniques that manipulate data (messages) so as to cipher or hide their existence. These techniques have several applications in technology and different connected fields: they're accustomed defend e-mail messages, mastercard data, company information, etc. a lot of specifically, steganography is that the art and science of communication during a manner that hides the existence of the communication. A steganographic system so embeds hidden content in ordinary cowl media thus as to not arouse associate degree eavesdropper's suspicion. As associate degree example, it's potential to engraft a text within a picture or associate degree audio file. On the opposite hand, cryptography is that the study of mathematical techniques associated with aspects of data security like confidentiality, information integrity, entity authentication, and information origin authentication. During this project we'll focus solely on confidentiality, i.e., the service accustomed keep the content of data from nearly those approved to possess it. Cryptography protects data by remodeling it into associate degree illegible format. it's helpful to attain confidential transmission over a public network. The initial text, or plaintext, is reborn into a coded equivalent known as cipher text via associate degree cryptography formula. Solely people who possess a secret key will decipher (decrypt) the cipher text into plaintext. Cryptography systems will be generally classified into symmetric-key systems that use one key (i.e., a password) that each the sender and therefore the receiver have, and public-key systems that use 2 keys, a public key known to everybody and a personal key that solely the recipient of messages uses.

The aim of each is to supply secret communication. Cryptography hides the contents of the message from associate degree assaulter, however not the existence of the message. Steganography/ watermarking even hide the terribly existence of the message within the communication information. Consequently, the idea of breaking the system is completely different for cryptosystems and stego systems (watermarking systems).

- A cryptanalytic system is broken once the assaulter will scan the secrete message.
- Breaking of a steganographic/watermarking system has 2 stages.

The assaulter will observe that Steganography/watermarking has been used. The assaulter {is able|is in a position|is scany} to read, modify or take away the hidden message.

A steganography/watermarking system is taken into account as insecure already if the detection of steganography/watermarking is feasible.

Visual Secret Sharing Scheme

The basic model of the visual cryptography consists of a many range of transparency sheets. On every transparency a cipher text is written that is indistinguishable from random noise. The hidden message is reconstructed by stacking a definite range of the transparencies and viewing them. The system are often utilized by anyone with none information of cryptography and while not playing any cryptographical computations. Naor and Shamir [8] have developed the Visual Secret Sharing theme (VSSS) to implement this model. In k out of n VSSS (which is additionally referred to as (k, n) scheme), a binary image (picture or text) is reworked into n sheets of transparencies of random pictures. The first image becomes visible once any k sheets of the n transparencies square measure place along, however any combination of but k sheets cannot reveal the first binary image. Within the theme, one element of the first

image is reproduced by m sub pixels on the sheets. The element is taken into account "on" (transparent) if the amount of clear sub pixels is quite a relentless threshold, and "off" if the clear sub pixel is a smaller amount than a relentless lower threshold, once the sheets square measure stacked along. The distinction α is that the distinction between the on and off threshold range of clear pixels. Ateniese et al. has extended the (k, n) VSSS to general access structures wherever senders will specify all qualified and verboten subsets of n participants. Droste thought of the matter of sharing quite one secret image among a collection of participants and planned a way to reconstruct totally {different|completely different} pictures with different Combination of sheets.

Extended Visual Cryptography

Extended Visual Cryptography could be a sort of cryptography that encodes variety of pictures within the approach that once the pictures on transparencies square measure stacked along, the hidden message seems while not a trace of original pictures. The decipherment is completed directly by the human sensory system with no special cryptographical calculations. Generally, visual cryptography suffers from the deterioration of the image quality. This project conjointly describes the tactic to enhance the standard of the output pictures. The trade-off between the image quality and therefore the security square measure mentioned and assessed by perceptive the particular results of this methodology. what is more, the optimisation of the image quality is mentioned. Naor ANd Shamir have mentioned an extension of the model that conceals the terribly existence of the key message. That is, every sheet carries some meaty pictures instead of random dots. They cited the (2, 2) example with the quantity of sub pixels m = 4. Ateniese has formalized this framework because the Extended Visual Cryptography and developed a theme for general access structures [Ateni01].They conjointly discuss the trade-off between the distinction of the every pictures on the sheets which of the ensuing image once stacked along in (k, k) cases.

Results

Initially the window appears like in the [Fig-3] and we have to select the secret image and the two cover images as shown here. After the selection of images click on the encryption there undergoes encoding of red, blue and green colours as shown in [Fig-4].

After encryption the secret image is hided beside the two cover images as shown in [Fig-5].

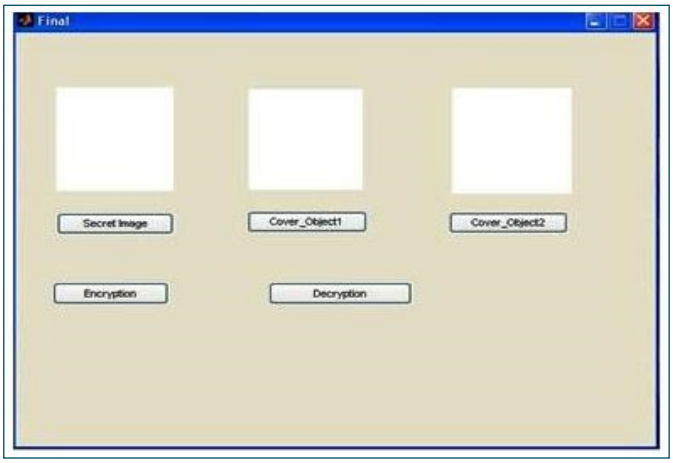

Fig. 3- Image selection

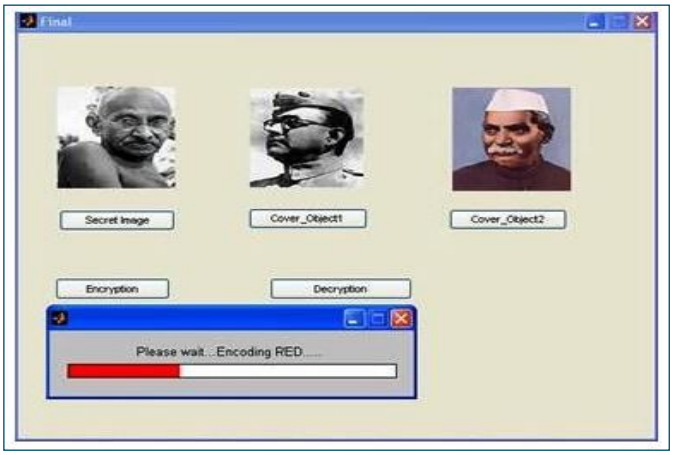

Fig. 4- Encryption image

Fig. 5- after encryption of secret image

To regain the secret image we need to decrypt the two cover images i.e. decoding red, blue and green.

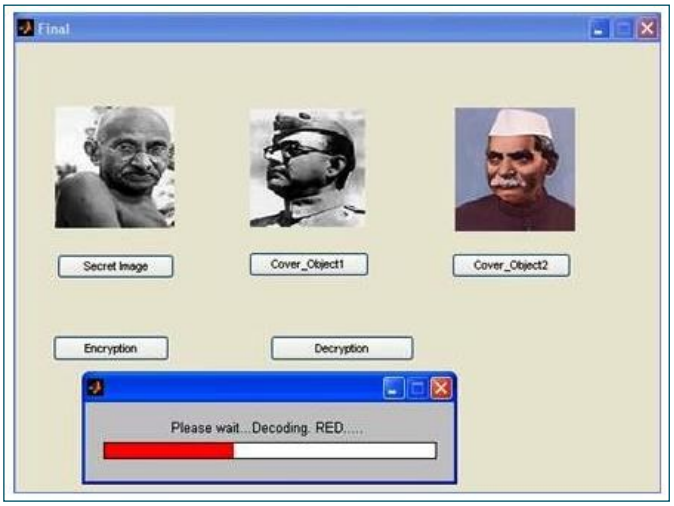

Fig. 6- Decrypting of secret image

Finally after decryption of red, green and blue colours we obtain the secret image which is as shown the [Fig-7].

Conclusion

This project planned the extended visual cryptography theme for

natural pictures. Next it showed a way to boost the image quality of the output by enhancing the image distinction on the far side the constraints given by the previous studies. the tactic permits the distinction improvement by extending the construct of error and by playacting 0.5 toning and secret writing at the same time. The trade -off between the image quality and therefore the security area unit assessed by perceptive the particular results of this technique. What is more, the optimisation of the image quality at a given distinction is mentioned. Below Associate in Nursing assumption that the prevalence of the violations is stochastically even within the pictures, a CFR operate is introduced for the image quality optimisation. The validity of the idea and therefore the result of image quality improvement are verified with the experiments. The higher than result shows that the given 3 input pictures and obtained the 2 output pictures that area unit combination of the third image. The third image is obtained by decrypting the 2 pictures.

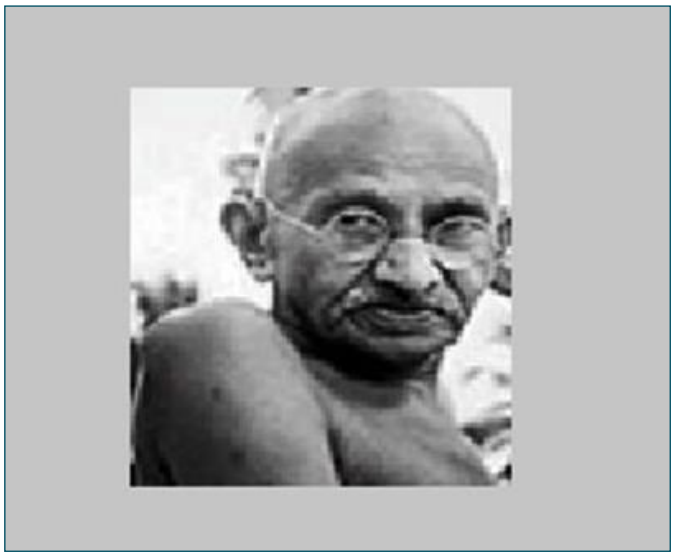

Fig. 7- Obtained secret image

Conflicts of Interest: None declared.

References

[1] Ateniese G., Blundo C., de Santis A. and Stinson D. (1996) *Information and Computation*, 129(2), 86-106.

[2] Ateniese G., Blundo C., De-Santis A. and Stinson D.R. (2001) *Theoretical Computer Science*, 250, 143-161.

[3] Verheul E.R. and van Tilborg H.C.A. (1997) *Design Codes and Cryptography*, 11(2), 179-196.

[4] Floyd R.W. and Steinberg L. (1997) *Proc. SID*, 17(2), 75-77.

[5] Gomes J. and Velho L. (1997) *Image Processing for Computer Graphics*, Springer.

[6] Hofmeister T., Krause M. and Simon H.U. (1997) *COCCON '97, Lecture Notes in Computer Science*, 1276, 176-185.

[7] Koga H. and Yamamoto H. (1995) *IEICE Transaction on Fundamentals*, E81-A(6), 1262-1269

[8] Naor M. and Shamir A. (1995) *Eurocrypt '94 Proceeding LNCS*, 950, 1-12.

[9] Naor M. and Shamir A. (1996) *Security Protocols*, 197-202.