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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Surreptitious Distribution for Color Image Using Haphazard Cycle

L.Devi[1], P.Neelambal[2]

Associate Professor, Department of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India [1]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: Visual cryptography may be a distinctive kind of secret writing procedure wherever illustration in cycle (Image, Text etc.) gets encrypted in such the way that coding is performed by Human sensory system with a computation free coding method. The beauty of the visual surreptitious sharing theme is in its coding method wherever with none complicated cryptanalytic computation encrypted knowledge is decrypted mistreatment individual Visual theme. However the secret writing technique wants cryptanalytic computation to divide the image into variety of elements. a visible cryptography theme may be a surreptitious distribution theme to write in code a surreptitious image in such the way that any qualified set of candidates will visually recovers the surreptitious image, whereas impermissible subsets haven't any data on SI. a visible recovery consists of Xeroxing the shares, that area unit gloom pictures, onto transparencies and heaping them one on the highest of the others. The participants in associate eligible set are able to see the surreptitious image with none information of cryptography and while not acting any cryptanalytic computation. Visual cryptography may be a powerful tool for instruction cryptography to general spectators. Applications have conjointly been projected to understand authentication, identification schemes and, recently, e choice schemes.

KEYWORDS: Visual cryptography, surreptitious image, Human sensory system.

I. INTRODUCTION

Visual cryptography may be a cryptanalytic technique wherever visual data (Image, text, etc.) gets encrypted in such the way that the coding is performed by the human sensory system while not aid of computers. Image may be a multimedia system element perceived by human perception. Picture element is that the smallest unit constructing a digital image. Every picture element of a thirty two bit digital color image area unit divided into four elements, specifically Alpha, Red, inexperienced and Blue; every with eight bits. Alpha half represents degree of transparency. If all bits of Alpha half area unit „0", then the image is absolutely clear during this paper we've got projected a surreptitious distribution rule to divide a digital color image into n range of shares wherever minimum k numbers of shares area unit comfortable to reconstruct the image. To attain this, following condition should be consummated. If there's „1" in sure position of a picture element, there should be „1" therein position of that exact picture element in (n−k) +1 range of shares generated from the first image. Within the remaining shares therein position of the actual picture element there's zero. In associate earlier try, we have a tendency to project a theme of generating (n-k) +1 distinct random ranges inside one to n to divide a picture into n number of shares. However that has to perform a range of iteration operations for every position of every picture element of every n number of shares if a „1" is found therein position. During this current work we've got projected a theme referred to as haphazard cycle that is a lot of generalized and offers relief from too several iteration operation.

In this Era, wherever distribution of knowledge became indispensable and is a component of most of the activities being performed on net. With the expansion of net the requirement for secure distribution of pictures has become extraordinarily necessary. There area unit essentially 2 necessary elements in cryptography, knowledge activity and secure transfer of knowledge. Visual Cryptography is associate rising theme that is proving to be economical for each problem with secure image distribution. This method is predicated on Human sensory system and therefore don't embrace complicated mathematical computations. The fundamental model of visual cryptography was

DOI: 10.15680/ijircce.2015. 0307149

given by Naor and Shami for Binary pictures. During this theme the surreptitious image is split into n range of shares out of that the sure range of shares (m) is shipped over the network to the desired destination, any m - one range of shares won't be able to reveal the surreptitious image. picture element is that the smallest unit of a picture .Here a thirty two - bit picture element of a digital image is taken and is split into Red, Green, Blue, and Alpha every of eight bit. Therefore four channel pictures area unit made wherever alpha half depicts the extent of transparency. In 1998, the lattice primarily based (k, n) VCS theme for grey level and color image was projected by H. Koga and H. Yamamoto. As per this technique the pixels area unit treated as parts of finite lattice and therefore the superimposing of pixels is completed as associate operation on the finite lattice. During this theme, (k, n) VCS for color pictures is represented with c colors as a group of c subsets in ordinal set of the finite lattice. Chin - Chen River projected spatial - domain image encrypting schemes. Here 2 surreptitious shares area unit embedded into 2 grey level pictures. To decrypt the hidden messages, close pictures is superimposed. Liguo Fang counseled a (2, n) theme supported equalization the performance between picture element enlargement and distinction. Xiaoping and Tan advised Threshold visual surreptitious distribution schemes that mixed XOR and OR operation and was supported binary linear error correcting code. In literature survey, we have a tendency to found that the disadvantage of those schemes is that solely single set of surreptitious messages is embedded, therefore for distribution great amount of surreptitious messages many shares ought to be generated and therefore the key should be sent firmly. the opposite problems area unit the drawback of enlargement within the size of decrypted image and therefore the quality of the decrypted image.

II. RELATED WORK

Noar and Shamir projected the primary visual surreptitious distribution theme of all in 1994. rather than the standard cryptanalytic strategies that need complicated computation, Noar and Shamir's theme uses the human sensory system to decipher the surreptitious image. What is more, the theme they projected may be a (k, n) threshold visual surreptitious distribution theme. In alternative words, this technique generates as several as n nonmeaningful pictures referred to as shares out of the surreptitious image, and to decrypt the surreptitious image needs as several as k , wherever k Љ n , or a lot of shares written out on transparencies and stacked along. Otherwise, there's no method the surreptitious image is unconcealed out of the shares. In a (2, 2)-threshold visual surreptitious distribution theme, let the surreptitious image be a binary image with size N × N. to start with, each picture element is extended into a 2×2 block, and every block consists of 2 black pixels and 2 white pixels. By bearing on a predefined secret writing table, a block is made by appreciate a connected picture element of the surreptitious image. Once all the surreptitious pixels area unit done processed, that's the instant the 2 shares area unit generated. Stacking the 2 shares along, we will reveal the surreptitious image. When the coding method, the scale of the shares becomes two N ×2 N. the subsequent area unit the surreptitious image picture element secret writing rules. First, the system at random picks one block from the six. oneto represent Share 1 block. Second, a picture element is found that conforms to the surreptitious image, and so the secret writing rules are compared so an identical block of Share two is generated. Once all the pixels area unit done processed, there'll be 2 two N ×2 N shares. Finally, stacking the 2 shares along, we will reveal the surreptitious image. As effective and ingenious as this theme is also, however, it will solely method one surreptitious image at a time, and therefore the surreptitious image will solely be either text or an easy black-and-white style.

The halftone technique is employed to translate the 3 color pictures into halftone pictures. Finally, by combining the 3 halftone pictures, a color halftone image is generated. Thecolor halftone image generation method. the color halftone image takes eight completely different colors to display: cyan, magenta, yellow, black, red, green, blue and white. The 3 strategies projected take the color halftone image because the surreptitious image. Here, we have a tendency to concentrate on the second technique and describe the small print of this technique. for every picture element of the color halftone image, the subsequent method should be done. First, 2×2 blocks area unit designed in step with Share one and therefore the four pixels C, M, Y and W area unit at random permuted. Then, the quantity of blocks is calculated for Share two in step with the colour magnitude relation of the four pixels with the secret writing table cited.

III. EXISTING SYSTEM

The concept of surreptitious distribution was severally projected by Adi Shamir and G. Blakley in 1979. In 1983 another technique of su distribution was projected by Asmuth and Bloom. Shamir‟ theme is predicated on

Polynomial Interpolation; Blakley theme is predicated on hyper geometry wherever as Asmuth- Bloom theme is predicated on Chinese Remainder theorem.

Shamir's Surreptitious Distribution theme

This technique is named (k, n) surreptitious distribution. The technique is represented with associate example within the following section. The (k, n) surreptitious distribution comes from the thought that k points area unit necessary to outline a polynomial of degree (k−1). To construct the polynomial, (k−1) coefficients a1, a2….ak−1 area unit needed. Here a0= S, the surreptitious knowledge. The polynomial f(x) = a0 + a1x + a2x2 + …..+ak−1xk−1 is made from the coefficients. Total n points let i=0…..n area unit taken and corresponding f(x) are calculated. From these values n range of pairs (i, f(i)) area unit created. the first coefficients area unit retrieved by interpolation technique from a minimum of k numbers of those pairs.

Blakley Surreptitious distribution theme

Blakley surreptitious distribution is predicated on hyper geometry. it's a general true that non-parallel planes run across at a particular purpose. This surreptitious distribution theme says that i) Surreptitious is purpose in m-dimensional house ii) Share corresponds to a hyper plane iii) Intersection of threshold planes provides the surreptitious iv) but threshold planes won't run across to the surreptitious.

IV. PROPOSED SYSTEM

The projected technique mistreatment haphazard cycle theme, turn out security to surreptitious image distribution. It will use multiple pictures in situ of binary image and generate the shares by visual cryptography technique. the wonder of the visual surreptitious distribution theme is in its coding method wherever with none complicated cryptanalytic computation encrypted knowledge is decrypted mistreatment Human sensory system (HVS). However the secret writing technique wants cryptanalytic computation to divide the image into variety of elements let n specified a minimum of a gaggle of k shares out of n shares reveals the surreptitious data, less of it'll reveal no data.

Advantages of proposed system:

This technique made complete security in image distribution and this method is extremely simple to implement and perceive by user.

V. IMPLEMENTATION

Haphazardcycle

In k-n surreptitious distribution theme a picture is split into n range of shares in such the way that the first image is retrieved by stacking at least k range of shares, where k n. If k range of shares area unit taken from n range of shares, the remaining shares area unit (n−k). The condition of inserting „1‟ within the specific bit position of a picture element in (n−k+1) shares should be consummated if the first image contains „1‟ within the specific bit position of the picture element. If seen from one aspect to the stacked shares, the bit cycle for a specific bit position of a picture element contains (n−k+1) range of „1‟ s and (k −1) numbers of „0‟s if the first image contains „1‟ within the particular bit position of the picture element. During this context this mix of „0‟ and „1‟ is taken as sequence. If a specific bit position contains „1‟, the sequence are one amongst nCk−1 completely different cycles.

Visual Cryptography Scheme Using Haphazard Cycle

A picture is taken as input. The range of shares the image would be divided (n) and number of shares to reconstruct the image (k) is additionally taken as input from user. The division is completed by the subsequent rule.
Step I: Take a picture IMG as input and calculate its dimension (w) and height (h).
Step II: Take the range of shares (n) and minimum number of shares (k) to be taken to reconstruct the image wherever k should be but or capable n. Calculate RECONS = (n-k)+1. Step III: produce a 3 dimensional array IMG_SHARE[n][w*h][32] to store the pixels of n range of shares. k-n surreptitious distribution visual cryptanalytic division is completed by the subsequent method.
for i = 0 to (w*h-1)

```
{
Scan each pixel value of IMG and convert it into 32 bit
binary string let PIX_ST.
for j = 0 to 31
{     if (PIX_ST.charAt(i) =1){
call Random_Place (n, RECONS)
}
for k = 0 to (RECONS−1)
{
Set IMG_SHARE [RAND[k]][i][j] = 1
}
}
}
Step IV: Create a one dimensional array IMG_CONS[n] to store constructed pixels of each n number of shares by the
following process.
for k1 = 0 to (n-1)
{For k2 = 0 to (w*h-1)
{String value= “”
for k3 = 0 to 31 {
value = value+IMG_SHARE [k1][k2][k3]
}
Construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0. Construct
pixel from these part and store it into IMG_CONS[k1].
}
Generate image from IMG_CONS [k1]1 [8].
}
```

Subroutine int Random_Place(n, RECONS)

```
{  Create an array RAND[RECONS] to store the
generated random number.
for i = 0 to (recons-1)
{
Generate a random number within n, let rand_int. [9]
if (rand_int is not in RAND [RECONS])
RAND [i] = rand_int
}
return RAND [RECONS]
}
```

Decryption Using Human Visual System.

It’s already mentioned that Human sensory system acts as associate OR perform. It’s conjointly mentioned that coding in Visual cryptography is completed by stacking k range of shares out of n shares generated. For pc generated coding method we've got used OR operation. The rule is represented below.

Step I: Take s range of shares ($s \geq k$) out of n range of shares generated.

Step II: for (i=1 to s)

little bit of every share, wherever one j w*h, to provide the ultimate image.}

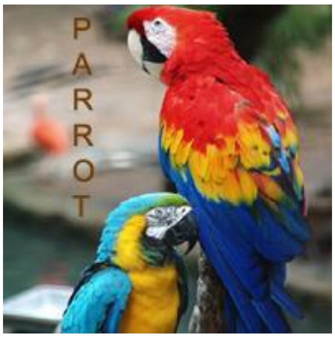
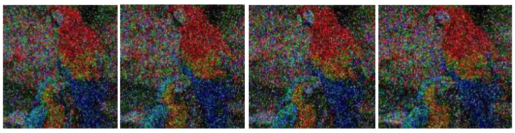


Fig 1 Source Image



Share1 Share2 share 3 share 4

Fig 2 Surreptitious shares for ‘Parrot’ image

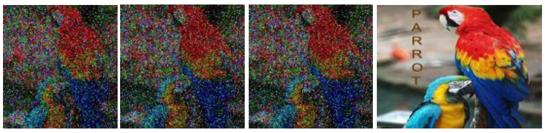


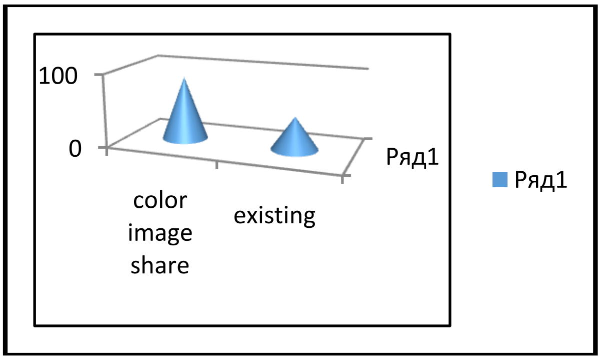
Fig 3 Retrieval of Parrot image

VI. Conclusion And Future Work

Here we've got projected k-n surreptitious distribution technique of color pictures mistreatment haphazard cycle. this method doesn't want complicated mathematical calculation just like the existing schemes. In each surreptitious share generation and coding half, OR operation is employed, that makes the theme terribly easy. However the most disadvantage of this theme, just like the alternative existing visual cryptography schemes is that the security. Somebody having sufficiently k range of shares will simply reconstruct the first image. During a future try we would like to supply some security themes to the projected technique to create the scheme safer.

Visual Cryptography technique is employed to safeguard image-based surreptitious data. During this theme we've got projected a way referred to as haphazard cycle to divide a picture into n range of shares. The shares area unit sent through completely different communication channels from sender to receiver so the chance of obtaining comfortable shares by the interloper minimizes. However the distorted shares could arise suspicion to the hacker’s mind that some surreptitious data is passed. The first image is encrypted employing a key to supply a lot of security to the current theme. The key is also a text or atiny low image. Steganography is utilized by close the surreptitious shares inside apparently innocent covers of digital image. This method is simpler in providing security from illicit attacks.

VII. Result Analysis



Security Analysis of Existing And Proposed

In surreptitious color image distribution provide high security by using the haphazard shares technique and algorithm than existing system methods.

References

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology-Eurocrypt"94, pp. 1–12, 1995.
[2] Ranjan Parekh, "Principles of Multimedia", TMH, 2006
[3] John F Koegel Buford, Multimedia Systems, Addison Wesley, 2000.
[4] Kandar Shyamalendu, Maiti Arnab, "K-N Surreptitious Sharing Visual Cryptography Scheme For Color Image Using Random Number", International Journal of Engineering Science and Technology, Vol.3 No. 3 March 2011, pp 1851-1857
[5] Kandar Shyamalendu, Maiti Arnab, "Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number", International Journal of Computer Application, Vol. 19 No. 4, April 2011. pp34s-39
[6] Kandar Shyamalendu, Maiti Arnab, Dhara Bibhas Chandra "Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking" International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, May 2011 pp543-549
[7] A. Shamir: "How to share a surreptitious ?" Comm ACM, 22(11):612-613, 1979.
[8] G. Blakley : "Safeguarding cryptographic keys " Proc. of AFIPS National Computer Conference, 1979.
[9] C. Asmuth and J. Bloom "A modular approach to key safeguarding" IEEE transaction on Information Theory, 29(2):208-210, 1983.
[10] Hartung F., Kuttter M., "Multimedia Watermarking Techniques", 1999 IEEE
[11] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications, 16(4):573–586, May 1998
[12] Nakajima M. , Yamaguchi Y., Extended visual cryptography for natural images. Journal of WSCG.v10 i2. 303-310.
[13] F. Liu, C. K. Wu, X.J. Lin, "Colour visual cryptography schemes" IET Information Security, 2008, Vol. 2, No. 4, pp. 151–165

BIOGRPHY

P.NEELAMBAL was born on 01.07.1989 in Tamilnadu, India. She received Master of Software Science 2011 degree from Erode Sengunthar Engineering College,Perundurai,Affiliated to Anna University-Chennai, Tamilnadu, India. She is Pursuing M.Phil (full time) degree from Muthayammal College of Arts & Science, in Periyar University Salem, Tamilnadu, India. She interested research area is Networking.

L.DEVICurrently doing Ph.D.Shereceived her B.sc Computer Science degree from Bharathidasan University and MCA., degree from BharathidasanUniversity.She has completed her M.Phil at Alagappa University. She is having 9 years of experience in collegiate teaching and she is the Associate Professor, Department of PG Computer Science in Muthayammal College of Arts and Science, Rasipuram affiliated by Periyar University. Her main research interests include Network security, Secured multiple path routing in MANET, P2P network IDS.

DOI: 10.15680/ijircce.2015. 0307149