ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

SECURE, STURDY AND PROGRESSIVE IMAGE SECRET SHARING VIA ERROR DIFFUSION IN HALFTONE VISUAL CRYPTOGRAPHY

Dr.F.Emerson Solomon and Dr.Kathir.Viswalingam*
*Professor, Dean R&D, R&D Division, Bharath University, Chennai.
Email: kvknowledge5252@gmail.com

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

Visual Cryptography is associate degree secret writing technique wherever a secret image is cryptographically encoded into shares. In visual secret sharing theme (k,n) the key pictures are often visually unconcealed by stacking along any k or a lot of transparencies of the shares and by inspecting but k shares one cannot retrieve the key image. Visual Secret Sharing supported halftone visual cryptography, the continuous-tone image is initial reworked into a halftone image, so encrypted victimisation visual secret sharing. In visual secret sharing schemes, pointless shares square measure encoded into halftone shares taking meaning visual data that reduces the suspicion of intruders. at the same time these halftone shares square measure error subtle to provide visually pleasing impact. Error diffusion is computationally economical and has low quality that produces halftone shares victimisation Floyd - cartoonist and Jarvis error filters to diffuse the error to the neighboring pixels. a technique of parallel error diffusion with complementary try halftone pictures to come up with sensible image quality is projected. Secret image is reconstructed by stacking qualified shares and it doesn't suffer from cross interference of share pictures.

Keywords: Visual Cryptography, Halftone visual cryptography, Parallel error diffusion, Error Diffusion, error filters.

1. Introduction

Security has become associate degree indivisible issue as data technology is ruling the planet currently. Cryptography is that the study of mathematical techniques and therefore the connected aspects of data security like confidentiality, information security, entity authentication and information origin authentication. Visual Cryptography (VC), projected by Naor et al. in [1], may be a cryptanalytic theme used for image secret writing. victimisation k-out-of- n visual secret sharing theme a secret image is encrypts into shares, that square measure pointless pictures , which will be transmitted or distributed over associate degree untrusted communicating. The properties of the human sensory system accustomed force the popularity of a secret message from overlapping shares, the key image is decrypted while not extra computations and not abundant data of cryptography. Every share resembles a random binary pattern. By inspecting but k shares, one cannot gain any data regarding the key image. In the case of 2-out-of-2 visual secret sharing shown in every element p taken from a secret binary image is encoded into a try of black and white subpixels in every of the two shares. If p is white or black one in every of row appointed for share one and share a pair of is chosen on a random basis with p=1/2 likelihood. the primary 2 subpixels during a row square measure appointed to share one out of {the 2|the a pair of} shares and therefore the succeeding two subpixels square measure appointed to share 2. Irrespective of whether or not a element is black or white, element p is encoded into 2 subpixels of equal chances. Therefore a personal share offers no clue as whether or not a element p is black or white. whereas superposition of the 2 shares as given in result column of the corresponding row , if the element p is white the superposition of the 2 shares outputs one white and one black subpixel such as a grey level of ½. Similarly, if p is black it leads to one in every of the 2 black subpixels, such as a grey level zero. Finally by stacking 2 shares along, we are able to acquire the total data of the key image. Naor et al. [1] proposes k out of n secret sharing theme to form shares. Blundo et al. [3] propose k-out-of-n theme to scale back the matter of distinction loss within the reconstructed pictures. associate degree access structure projected in Ateniese et al. [3] consists of all the qualified and out subsets of shares. The k-out-of-n theme is healthier with regard to element growth than [1] however restricted solely to binary image. Later Chang Jiang &amp; Hsiang [4] proposes visual cryptography supported visual secret sharing that conjointly been extended to a greyscale secret image by victimisation video digitizing techniques to convert gray level pictures into binary pictures. Ateniese et al. developed the tactic of Extended Visual Cryptography within which the shares not solely contain the key data, however also are themselves meaning halftone pictures. Nakajima any extended the Extended Visual Cryptography approach for natural grayscale image with patterns carrying visual data. however shares generated was of poor quality that once more will increase the suspicion of information secret writing as in [6]. Zhou dynasty and Arce [7],[8] proposes halftone visual cryptography to extend the standard of the meaning shares supported the principle of void and cluster video digitizing. However within the void and cluster algorithmic rule to switch the element within the original halftone image obsessed on the content of the element chosen which can end in visible image residual options of the first halftone pictures.

Visual Cryptography supported halftoning, the continuous-tone image is initial reworked into a halftone image, so the visual secret sharing is applied. Halftoning uses patterns of larger and smaller pixels during a monochrome pictures to provide the illusion of grey i.e., method of changing a grey scale image into a binary image. Most typical halftoning ways square measure classical screening, video digitizing with blue noise, direct binary search, error diffusion [2]. Error diffusion may be a new methodology of image halftoning that turn out abundant higher quality pictures with less computation value. The algorithmic rule depends on dispersive the division error from thresholding to neighbors of the present element once the image is scanned in formation fashion. Thus, visually pleasing halftone shares are often obtained. Parallel error diffusion victimisation halftone visual cryptography proposes in [2] may be a new suggests that of changing a secret image into meaning shares. Grayscale image to be halftoned have to be compelled to be designated fittingly. therefore a complementary try is utilized to realize higher image quality. Secret data pixels are often encoded into the at the same time halftoned grayscale pictures and error diffusion diffuses the division error within the halftoned image victimisation applicable error filter to its neighboring pixels while not dynamic the planned pixels.

2. Related Work

Visual cryptography may be a cryptanalytic technique that permits visual data (pictures, text, etc.) to be encrypted in such the way that the cryptography are often performed by humans while not the help computers. the subsequent section give associate degree introduction to visual secret sharing theme, halftone visual cryptography and error diffusion

A. Visual Secret Sharing Theme

Visual Secret Sharing is predicated on the access structure schemes such that as follows :

2 out of two theme (2 sub pixels) : during this theme, a black and white image element divided in 2 sub-pixels out of that arbitrarily chosen between black and white betting on the present element . If the image element is white, then arbitrarily opt for one in every of the 2 rows for white else if it's black, then arbitrarily choose from one in every of the 2 rows for black. A random column-permutation of white element and black element is completed from S0 and S1 to come up with a given matrix as C0 and C1 represents white and black element severally that produces 2 vectors V0 and V1 such as prevalence of the element i.e.. either white or black during a secret image. If white then V0 are going to be outputted that is of either 01 or ten with gray-level ½ and if black element then V1 are going to be outputted with either eleven or eleven. 2 out of two theme (4 subpixels): during this theme, every element black/white encoded as a a pair ofx2 cell in 2 shares (key and cipher) wherever every share has 2 black, a pair of clear subpixels. Once stacked, shares mix to provide solid black or 0.5 black (seen as grey).Here C0 and C1 square measure the 2

column matrices of white and black element severally that is chosen on random basis. 3 out of 3 Scheme: This theme encrypts the key image into 3 shares such only all three shares square measure combined, the key image are going to be unconcealed. Basic visual cryptography supported breaking of elements into sub-pixels or pixel growth is performed. Let P = be a group of components known as participants, and let 2P denote the set of all subsets of P. Let ΓQual a pair of P and ΓForb 2P, wherever ΓQual ∩ ΓForb =Ø. The members of ΓQual square measure qualified sets and members of ΓForb square measure out sets. The try (ΓQual, ΓForb) is named the access structure of the theme. Any qualified set of participants in X ϵ ΓQual will visually decipher secret image, however a out set of participants has no data Y ϵ ΓForb. therefore ΓQual {is known as|is named|is termed} monotone increasing whereas ϵ ΓForb called monotone decreasing. The participants square measure able to observe the key image while not activity any cryptanalytic computation. Visual secret sharing is predicated on 2 parameters: the pixels growth γ , that is that the range of sub elements on every share that every pixel of the key image is encoded into, and therefore the distinction α, that is that the measure of the distinction of a black element and a white element within the reconstructed image. In the case wherever ΓQual is monotone increasing, ΓForb is monotone decreasing, and ΓQual U ΓForb =2P, the access structure is alleged to be robust. The message consists of black and white pixels. every element seems in n shares, one for every transparency. every share may be a assortment of m black and white subpixels. The ensuing structure are often represented by associate degree [n x m] Boolean matrix S = [sij] wherever sij=1 iff the jth subpixel within the ith transparency is black. thus the gray level of the combined share is obtained by stacking the transparencies during a during a participant set X=, is proportional to the performing weight w(V) of the m-vector V=OR(ri1,….,ris) wherever ri1 , ..., ris square measure the rows of matrix S related to the transparencies that square measure stacked. This gray level is taken by the sensory system of the users as black or as white in according with some rule of distinction. Definition: Let (ΓQual, ΓForb) be associate degree access structure on a group of n participants. 2 collections of [n x m] Boolean matrices b0 and b1 represent a visible cryptography theme (Γ Qual, ΓForb, m) if there exist the worth α(m) and therefore the set xϵ Γ Qual satisfying:

1. Any (qualified) set X= X ϵ Γ Qual will recover the shared image by stacking their transparencies. Formally, for any M ϵ b0, the “or” V of rows i1 , i2 , ..., IP satisfies w(V) ≤ Texas – α(m).m; whereas, for any M ϵ b1 it results that w(V) ≥ Texas.
2. Any (forbidden) set X= ϵ ΓForb has no data on the shared image. Formally, the 2 collections of p x m matrices Dt , with t ϵ , obtained by proscribing every n x m matrix in bt to rows i1 , i2 , ..., IP square measure indistinguishable

within the sense that they contain constant matrices with constant frequencies. Each element p of the first image are going to be encoded into n shares, every of that consists of m subpixels. whereas distributing a share, a white (black, resp.) element arbitrarily opt for one in every of the matrices in S0 (S1, resp.), and distribute row i to participant i. The chosen matrix defines the m subpixels in every of the n transparencies. The property of distinction of the image states that once a certified set of users stack their transparencies they'll properly recover the shared image. the worth α(m) is named relative distinction, the amount α(m) wherever m is observed because the distinction of the image, the set X ϵ ΓQual is named the set of thresholds, and Texas is that the threshold related to X ϵ Γ Qual. The distinction has got to be massive as attainable and a minimum of one, that is, α(m) ≥ 1/m. The another property is named security, since it implies that, even by inspecting all their shares, a out set of participants cannot gain any data helpful to decide whether or not the shared element was white or black.

B. Halftone Visual Cryptography

Halftone Visual Cryptography was introduced in [2],[7],[8] and is constructed upon the idea matrices collections out there in typical visual cryptography. A secret binary element p in halftone visual cryptography is encoded into associate degree array of q=v1*v2 known as a halftone cell, in every of the n shares. the choice of the key data pixels during a halftone cell is vital because it affects the visual quality of the resultant halftone shares. However, as long because the positions of the key data pixels square measure freelance of the key data, the arrangement of the changed pixels satisfies the safety needs. To get higher visual results, the error diffusion algorithmic rule [2] accustomed win improved halftone image quality in every share. The error diffusion algorithmic rule uses a Floyd or Jarvis error filter given . a pair of to diffuse the error during a halftone image to its neighboring pixels to supply visually pleasing image while not modifying the planned secret data pixels. a pair of (a) represents a Floyd - cartoonist error filter with a weightage of sixteen that is distributed as h (0,1) = 7/16, h(1,-1) = 3/16, h (1,0) = 5/16 and h (1,1) = 1/16 to its four neighboring pixels. Current element is assumed to be at position h(0,0). a pair of (b) represents a Jarvis error filter with a weightage of forty eight that is distributed to its twelve neighboring pixels.

C. Error Diffusion

Error diffusion may be a straightforward, nonetheless economical algorithmic rule to halftone a grayscale image compared with alternative halftoning algorithms. The division error at every element is filtered and fed-back to a group of future input pixels. shows a binary error diffusion diagram wherever f(m,n) represents the (m.n)th element of the input grayscale image, d(m,n) is that the input to the brink block t(m,n) and g(m,n) is that the output quantity element price that is either one or zero. Error diffusion consists of 2 main elements out of that the primary element is that the threshold block t(m,n) and another is that the error filter h(k,l) .

Algorithm for error diffusion:-

1) Start with $d(m,n) = f(m,n)$

2) Scan pixels in image during a planned order so move to step three.

3) Generate element g(m,n) supported threshold condition as follows:

if d(m,n) &gt; t(m,n) g(m,n) = 0 , if d(m,n) ≤ t(m,n)

4) Compute division error $e(m,n) = g(m,n) - d(m,n)$

5) Diffuse the error victimisation error filter h(k,l) to the neighboring pixels and reason the input to the brink block victimisation $d(m,n) = f(m,n) - \sum h(k,l)*e(m-k,n-l)$

6) Continue the method till all the errors square measure subtle until it reaches to the sides.

3. Our Work

Parallel error diffusion proposes in [2] is combined with complementary try halftone shares to yield sensible image quality. This methodology consists of the subsequent modules:-

a) Share Creation

The halftone visual cryptography divides a share image to non-overlapping halftone cell of size q=v1*v2 and secret image element encoded to the halftone cell wherever every cell consists of γ SIPs and (q- γ) non-SIPs of ‘q’ pixels. Pixels that carry the key image data square measure planned before a halftone share is generated. Rather than modifying halftone pictures to encrypt secret data, it's shown that it's viable to at the same time halftone grayscale pictures and encodes the key data into the halftone pictures. These pixels square measure then naturally embedded into the halftone shares once the grayscale pictures square measure halftoned. SIP distributed homogenously with peak separation from one another to achieve sensible image quality and arbitrarily distributed to make sure security can transmission through communicating.

b) Halftoning Grayscale Image

Halftoning method converts a continuous-tone image (grayscale image) into a binary valued image victimisation halftoning algorithmic rule like Error diffusion or Direct binary search. Error diffusion is computationally economical than direct binary search therefore it's used for halftone a image. This method uses the concept of victimisation patterns of larger and smaller pixels during a monochrome pictures to provide the illusion of grey i.e., method of changing a grey scale image into a binary image. Using the key image and multiple grayscale pictures, halftone shares square measure generated such the resultant halftone shares aren't any longer random patterns, however take meaning visual pictures. A secret binary element p is applied with visual secret sharing element growth to come up with γ subpixels that is generated on random basis from matrix collections C0 and C1. Then the γ subpixels square measure encoded into a block of the halftoned image of size q=v1*v2, observed as a halftone cell, in every of the n shares.

The size of the share image is 512 x 512 and therefore the secret image is of size 128 x 128. In parallel error diffusion halftoning of grayscale image can generate sufficient range of black pixels to dam share visual data to look on the reconstructed image. Insertion of the black element restricted to attenuate visible distortions. The choice of the key data pixels during a halftone cell is vital because it affects the visual quality of the resultant halftone shares. By combining parallel error diffusion [2] with complementary share try [8] can yield sensible quality image.

Algorithm:

1. Choose a secret image SI to be encrypted.
2. Choose a grayscale image GI to be halftoned.
3. Apply error diffusion victimisation applicable error filter and generate the halftoned image I.
4. From I generate the corresponding complemented image I’ by reversing white/black pixels.
5. Contemplate I as Share1, it is distributed to Participant1 and equally, I’ as Share2 to Participant2.
6. Encrypt the element p to v1*v2 halftone cell were solely cells square measure secret data pixels and alternative pixels carry visual data known as as standard pixels.
7. Choice of subpixels is arbitrarily done from C0, C1 matrix wherever row i of a matix is distributed to halftoned image I and row j to complemented halftoned image I’.
8. Secret pixels square measure encoded to the planned position in I and I’.

However, as long because the positions of the key data pixels square measure freelance of the key data, the arrangement of the changed pixels satisfies the safety needs. to get higher visual results, the error diffusion algorithmic rule [2] accustomed win improved halftone image quality in every share.

c) Error Diffusion

Error diffusion an easy and wide used halftone methodology that yields an honest compromise between the image quality and therefore the machine quality. Error diffusion halftones the input grayscale pictures however doesn't modification the planned pixels. once halftoning a grayscale image, error diffusion diffuses away the division error into the neighboring grayscale pixels in order that a visually pleasing halftone image is obtained. during this approach coding of the key data imposes further constraints on the error diffusion. However, the extra division error introduced by the coding of the key data pixels is subtle away by error diffusion to the neighboring grayscale pixels within the direction of the scan as given .Thus, visually pleasing halftone shares are often obtained.

Other ways like auxiliary black pixels [2] also are accustomed permit the reconstructed image resistant to the interference from the share pictures. altogether ways, non-relevant visual data is prevented from showing on the reconstructed image and therefore the same distinction over the whole reconstructed image is achieved, resulting in correct interpretation of the decoded image. The projected halftone VSS construction ways square measure computationally economical and, as verified by in depth simulations, will turn out visually pleasing halftone shares that applied to visual secret writing and visual authentication .

The security of the made halftone VSS theme is bonded by the safety of the underlying VSS theme. Secret image pixels that is split into shares is encoded into a halftone grayscale image. if the element is non-secret data element then it's suffered a error filter h (k,l) as given four to diffuse the error e(m,n). if the element is secret data element g(m,n) is up to the worth of the pre-determined secret data pixels. Error e(m,n) is calculated because the input to the thresholding block and therefore the price of the key data element.

d) Stacking

In the methodology projected during this paper, {a massive|an outsized|an oversized} HVC growth is fascinating to create the standard index large. however the distinction loss of the decoded image is severe once the halftone VC growth is massive. However, a coffee distinction doesn't hinder the coding of the key image if the coding are often performed digitally. Shares square measure alleged to be derived on transparencies and coding of the key image involves stacking the shares physically by suggests that of OR operation five shows the stacking of 2 halftone cells of size Q = four were A and B square measure secret data pixels that remains same for each the halftone cells. five(a) and five(b) represents white element whereas 5 (c) and 5 (d) represents black element. Reconstruction of the white element is with distinction of 1/v1*v2.

4. Conclusion

During this methodology of parallel error diffusion method combined with complementary share try is projected to boost the image quality of the halftone shares. The halftoning visual cryptanalytic methodology inserts the pixels carrying secret data into antecedent uncoded halftone shares. Visual cryptography is employed beside the construct of halftoning wherever the continuous-tone image is initial reworked into a binary image, so the visual secret sharing is applied. the key image is encoded into halftone shares taking meaning visual data by at the same time victimisation error diffusion to halftone shares. Error diffusion has low quality and provides halftone shares with sensible image quality. A reconstructed secret image, obtained by stacking qualified shares along, doesn't suffer from cross interference of share pictures.

References

1. M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptograhy:EUROCRYPT’94, LNCS, vol. 950, pp. 1–12, 1995.
2. Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography via Error Diffusion,” IEEE Trans. on data Forensics And Security, Vol. 4, No. 3. , Sep. 2009
3. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptography for general access structures,” Inf. Comput., vol. 129, no. 2, pp. 86–106, Sep. 1996.
4. C. C. Lin and W. H. Tsai, “Visual cryptography for gray-level pictures by video digitizing techniques,” Pattern Recognit. Lett., vol. 24, pp. 349–358, Jan. 2003.
5. Abhishek Parakh, Subhash Kak, “A algorithmic Threshold Visual Cryptography Scheme” CoRR abs/0902.2487, Feb. 2009
6. M. Nakajima and Y. Yamaguchi, “Extended visual cryptography for natural pictures,” J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.
7. Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” in Proc. IEEE Int. Conf. Image method., Barcelona, Spain, Sep. 2003.
8. Z. Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image method., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
9. Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S, “An summary of visual cryptography ”, International Journal of machine Intelligence Techniques, Vol. 1, Issue 1, PP. 32-37., 2010
10. P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, “Survey of Visual Cryptography Schemes,” International Journal of Security and Its Applications Vol. 4, No. 2, April. 2010.