International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 7 1790 – 1793

Separable Reversible Knowledge Activity in Encrypted Image with Compression of Knowledge and Image

D. Anithamma
Dept. of CSE
Intell engineering college,
Ananthapuramu, AP, India.
anitha.d43@gmail.com

D. Lakshmi Narayana Reddy
Assistant Professor, Dept. of CSE
Intell engineering College
Ananthapuramu, AP, India
lakshmi1217@gmail.com

Abstract: Since many years, the protection of multimedia system knowledge is changing into vital. The protections of this multimedia system knowledge are often finished cryptography or knowledge concealment algorithms. To decrease the UTC, the information compression is critical. Since few years, a brand new downside is making an attempt to mix in a very single step, compression, and cryptography and knowledge concealment. So far, few solutions are projected to mix image cryptography and compression as an example. Nowadays, a brand new challenge consists to enter knowledge in encrypted pictures. Since the entropy of encrypted image is peak, the embedding step, thought-about like noise, isn't doable by mistreatment customary knowledge concealment algorithms. A brand new plan is to use reversible knowledge concealment algorithms on encrypted pictures by want to get rid of the embedded knowledge before the image cryptography. Recent reversible knowledge concealment strategies are projected with high capability, however these strategies aren't applicable on encrypted pictures. During this paper we tend to propose Associate in nursing analysis of the native variance of the marked encrypted pictures so as to get rid of the embedded knowledge throughout the cryptography step. We've got applied our methodology on varied pictures, and that we show and analyze the obtained results.

Keywords: *multimedia data, encryption, data hiding, Embed data, De-embed data, Compression.*

******

I. INTRODUCTION

The amount of digital pictures has enhanced chop-chop on the web. Image security becomes more and more necessary for several applications, e.g., confidential transmission, video police work, military and medical applications. for instance, the need of quick and secure diagnosing is significant within the medical world.1, 2 Nowadays, the transmission of pictures may be a daily routine associated it's necessary to find an efficient thanks to transmit them over networks. To decrease the transmission time, the information compression is critical. The protection of this transmission information is finished coding or information concealment algorithms. Since few years, a tangle is to undertake to mix compression, coding and information concealment in a very single step. For instance, some solutions were projected in to mix image coding and compression. 2 main teams of technologies are developed for this purpose. The first one is primarily based on content protection through coding. There are many ways to cipher binary pictures or grey level pictures.3–6 during this cluster, correct decipherment of information needs a key. The second cluster bases the protection on digital watermarking or information concealment, aimed toward on the Q.T. embedding a message into the information.7, eight These 2 technologies is used complementary9, ten and reciprocally independent.11 Sinha and Singh projected a method to cipher a picture for secure image transmission.12 In their approach the digital signature of the first image is extra to the encoded version of the first image. The coding of the image is completed victimization associate applicable error management code. At the receiver finish, once the decipherment of the image, the digital signature is accustomed verify the legitimacy of the image. Coding and watermarking algorithmic rules have confidence the Kerckhoffs principle13: all the small print of the algorithm is notable, and solely the key to cipher and rewrite the information ought to be secret.

Nowadays, a replacement challenge consists to implant information in encrypted pictures. Previous work projected to implant information in associate encrypted image by victimization associate irreversible approach of information concealment.14 the challenge was to find associate coding technique sturdy to noise. Since the entropy of encrypted image is greatest, the embedding step, thought of like noise, isn't doable by victimization normal information concealment algorithms. a replacement plan is to use reversible information concealment algorithms on encrypted pictures by desire to get rid of the embedded information before the image decipherment. Recent reversible information concealment ways are projected with high capability, 15, sixteen however these ways don't seem to be applicable on encrypted pictures. During this paper we have a tendency to propose associate analysis of the native variance of the marked encrypted pictures so as to get rid of the embedded information throughout the decipherment step. The rest of the paper is organized as follows. Section 2 presents the principle of image encryption by using Triple DES algorithm and details the proposed reversible data hiding method for encrypted images. In Section 3, we show and analyze results of the proposed method applied to real images. Conclusion is finally drawn in Section 4.

II. PROPOSED METHOD

A. *IMAGE ENCRYPTION*

The use of pc networks for information transmissions has created the requirement of security. several strong message secret writing techniques are developed to produce this demand. The secret writing method is even, uneven or hybrid17 and might be applied to blocks or streams.18–20 many uneven algorithms use long keys to confirm the confidentiality as a result of a locality of the secret is glorious. These algorithms aren't applicable enough to be applied to photographs as a result of they need a high machine quality. Within the case of block secret writing ways applied to photographs, one will encounter 3 inconveniences. The first one is after we have same zones (regions with identical color), all blocks within these zones are encrypted in the same manner. The second downside is that block secret writing ways aren't strong to noise. Indeed, thanks to the massive size of the blocks (which is a minimum of 128 bits) the secret writing algorithms per block, even or uneven, cannot be strong to noise. The third downside is information integrity. The mix of secret writing and data-hiding will solve these forms of issues.

Triple DES is another mode of DES operation. It takes 3 64-bit keys, for AN overall key length of 192 bits. In Stealth, you merely kind within the entire 192-bit (24 character) key instead of getting into every of the 3 keys severally. The Triple DES DLL then breaks the user-provided key into 3 sub keys, artifact the keys if necessary in order that they area unit every sixty four bits long. The procedure for encoding is strictly an equivalent as regular DES, however it's recurrent 3 times, thence the name Triple DES. the information is encrypted with the primary key, decrypted with the second key, and eventually encrypted once more with the third key.

Triple DES runs 3 times slower than DES, however is way safer if used properly. The procedure for decrypting one thing is that the same because the procedure for encoding, except it's dead in reverse. Like DES, knowledge is encrypted and decrypted in 64-bit chunks. though the input key for DES is sixty four bits long, the particular key utilized by DES is just fifty six bits long. the smallest amount important (right-most) bit in every computer memory unit could be a parity, and may be set in order that there area unit continually AN odd variety of 1s in each computer memory unit. These parity bits area unit unheeded, thus solely the seven most important bits of every computer memory unit area unit used, leading to a key length of fifty six bits. this suggests that the effective key strength for Triple DES is truly 168 bits as a result of every of the 3 keys contains eight parity bits that aren't used throughout the encoding method.

The Triple DES formula will support many cipher modes: ECB (Electronic Code Book), blood profile (Cipher Block Chaining), The ECB mode is truly the essential Triple DES formula. With the ECB mode, every plaintext block Xi is encrypted with an equivalent secret key k manufacturing the cipher text block Yi:

$$Yi = Ek(Xi). \quad (1)$$

The CBC mode adds a feedback mechanism to a block cipher. every cipher text block Loloish is XORed with the incoming plaintext block Xi+1 before being encrypted with the key k. Associate in Nursing initialisation vector (IV) is employed for the first iteration. In fact, all modes (except the ECB mode) need the employment of Associate in Nursing IV. In CFB mode, Y0 is substituted by the IV. The key stream component Zi is then generated and also the cipher text block Loloish is made. though Triple DES may be a block cipher, within the CFB mode it operates as a stream cipher. These modes don't need any special measures to handle messages whose lengths don't seem to be multiples of the block size since all of them work by XORing the plaintext with the output of the block cipher. every mode has its blessings and drawbacks. as an example in ECB and mode, any modification within the plaintext block Xi causes the corresponding ciphered block Loloish to be altered, however alternative ciphered blocks don't seem to be affected. On the opposite hand, if a plaintext block Xi is modified in CBC and mode, then Loloish and every one consequent ciphered blocks are affected. These properties mean that CBC mode ar helpful for the aim of authentication whereas ECB mode treat severally every block.

In this paper, for the planned technique, the ECB mode of Triple DES algorithmic program has been chosen to inscribe the photographs. the photographs ar therefore encrypted by blocks of (128 bits or 192 bits) that correspond to sixteen grey level pixels. we will first live the image info content with the entropy H(X). If a picture X has M grey levels $\alpha(4)$ with zero $\leq (4) <$ M, and also the likelihood of grey level $\alpha(4)$ is P($\alpha(4)$), the entropy H(X), while not considering the correlation of grey levels.

If the secret writing algorithmic program is efficient, the entropy H(Y) of Associate in Nursing encrypted image Y should be peak so larger than the entropy H(X) of the initial image X:$H(Y) \geq H(X)$.(2)

B. *Encoding algorithm*

The writing rule consists of 2 steps that ar the coding and therefore the information concealment step. for every block Xi composed of n pixels pj of a picture of N pixels, we have a tendency to apply the Triple DES coding rule by block:

$$Yi = Ek(Xi) \quad .(3)$$

Where Ek() is that the coding perform with the key key k and Lolo is that the corresponding cipher-text to Xi. One will note that the sizes of Xi and Lolo ar identical. throughout the info concealment step, in every cipher-text we have a tendency to modify just one little bit of one encrypted component of Yi:

$$Y\ WI = DHk\ (Yi), \quad (4)$$

Where DHk() is that the information concealment perform WIth the key key k and Y wi is that the marked cipher-text. we have a tendency to used bit substitution-based information concealment methodology so as to infix the bits

of the hidden message. for every block Lolo, the key key k is employed because the seed of the pseudo-random variety generator (PRNG) to substitute the little bit of a component with the bit to hidden. At the tip of the writing method we have a tendency to get a marked encrypted image. Since we have a tendency to infix one bit in every block of n pixels, the embedding issue is adequate 1/n bit per component.

C. Decoding algorithm

Where DHk () is that the information activity perform American stateth the key key k and Y wi is that the marked cipher-text. we tend to used bit substitution-based information activity technique so as to plant the bits of the hidden message. for every block Yi, the key key k is employed because the seed of the pseudo-random range generator (PRNG) to substitute the little bit of a pel with the bit to hidden. At the top of the cryptography method we tend to get a marked encrypted image. Since we tend to plant one bit in every block of n pixels, the embedding issue is up to 1/n bit per pel The decipherment rule is additionally composed of 2 steps that square measure the extraction of the message and also the decipherment removing.

The extraction of the message is extremely simple: it's barely enough to scan the bits of the pixels we've marked by victimization the key key k and also the same PRNG. however once the extraction, every marked cipher-text remains marked. the matter is then to rewrite the marked encrypted image. The decipherment removing is completed by analyzing the native variance throughout the decipherment of the marked encrypted pictures.

For each marked cipher-text Y American state we tend to apply the decipherment perform Dk() for the 2 attainable values of the hidden bit (0 or 1) and that we analyze the native variance of the 2 decrypted blocks X0i and X1i. within the encrypted image, the entropy should be peak and bigger than the first one as delineated in Equation(3). Moreover, the native variance of the encrypted image is beyond for an ingenious image. From this assumption we tend to determined to check for every block the native variance of X0i with X1i and that we choose the bit price wherever the native variance is that the smaller.

III EXPERIMENTAL RESULTS

We have applied our method on various gray level images and we show the results of the proposed method applied on a medical image (1024 × 1024 pixels) illustrated in Fig. 1.a and the image of Baboon (512 × 512 pixels), We have encrypted the original image Fig. 1.a by using the Triple DES algorithm in ECB mode to get the encrypted image illustrated in Fig. 4.b. The size of the blocks is 16 pixels (128 or 192 bits). From this encrypted **i**mage we have then embedded 65536 bits to get the marked and encrypted image illustrated in Fig. 1.c. The image difference between the Fig. 1.b and c is illustrated in the Fig. 1.d. We can see the pixels where we have substituted one bit with the message. The PSNR of the marked and encrypted image illustrated in Fig. 1.c equals to 66.13 dB. In Fig. 1.b and c, one can notice that the initial information is not visible anymore. By comparing the histogram of the initial image, with that of the encrypted image, we notice that the probabilities of appearance of every grey level are equitably distributed. The histogram of the encrypted image is flat, and from equation (2) we get very high entropy H(Y) of 7.997 bits/pixel (H(X) = 7.216 bits/pixel for the original image). The information redundancy is very small **and** thus statistical attacks would be difficult.22 From equation (6) we also analyzed the variation of the local standard deviation σ for each pixel while taking its neighbors into account. The mean local standard deviation is equal to 68.278 gray levels for the marked encrypted image illustrated Fig. 1.c (the mean local standard deviation is equal to 1.349 gray levels for the original medical image Fig. 1.a.).

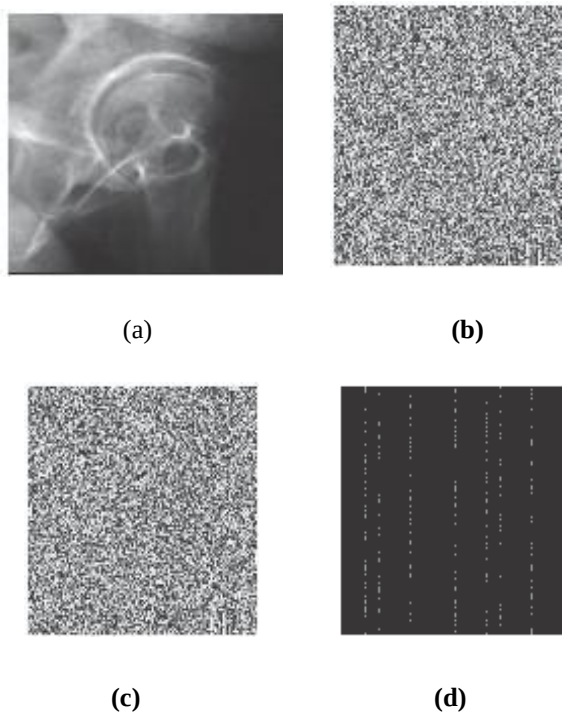

Figure 1. a) Original medical image of 1024 × 1024 pixels, b) Encrypted image with Triple DES in ECB mode, c) Encrypted and marked image with 65536 hidden bits, d) Difference between b) and c).

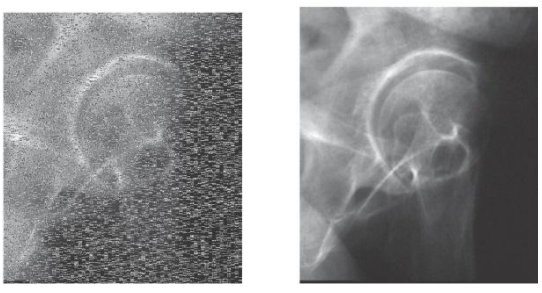

Figure 2. a) Extraction of the message and decryption of the marked image Fig 1.c, b) Decryption and deleting of the message by using the proposed method.

For the decoding process, after the message extraction, if we apply only the decryption on the image of Fig. 1.c, we get

the image illustrated in Fig. 6.a. The histogram of this decrypted image, Even if this histogram looks similar to the original one, the quality of this decrypted image is very bad and its PSNR equals to 13.27 dB. The mean local standard deviation is equal to 34.010 gray levels for this image, and its local standard deviation By analyzing the local standard deviation for each block during the decryption step we are able to find the original value of each bit and thus to remove the hidden data. The application of the equation during the decryption step allows us to get the decrypted image illustrated in Fig. 2.b. This decrypted image is exactly the original image with a PSNR = ∞.

CONCLUSION

In conclusion, during this paper exploitation Triple DES algorithmic program is employed to beat the brute force attack once reversible knowledge concealment is enforced within the networks with our projected reversible knowledge concealment methodology for encrypted pictures we tend to are ready to imbed knowledge in encrypted pictures and so to decipher the image and to make the first image by removing the hidden knowledge. During this paper, we tend to careful all the steps of the projected methodology and that we illustrated the tactic with schemes. we tend to given and analyzed varied results by showing the plots of the native normal deviations. Within the projected methodology, the embedding issue is one bit for sixteen pixels. This tiny price of the embedding issue is barely is to possess to decide on between two values for every block throughout the coding. For the long run, we tend to are thinking to enhance this methodology by increasing the payload however additionally the quality.

REFERENCES

[1] J. Bernarding, A. Thiel, and A. Grzesik, "A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encrytion," International Journal of Medical Informatics 64, pp. 429–438, 2001.

[2] 2. R. Norcen, M. Podesser, A. Pommer, H. Schmidt, and A. Uhl, "Confidential Storage and Transmission of Medical Image Data," Computers in Biology and Medicine 33, pp. 277–292, 2003.

[3] A. Uhl and A. Pommer, Image and Video Encryption: From Digital Rights Management to Secured Personal Communication, Springer, 2005.

[4] K. Chung and L. Chang, "Large encrypting binary images with higher security," Pattern Recognition Letters 19, pp. 461–468, 1998.

[5] C. Chang, M. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," The Journal of Systems and Software 58, pp. 83–91, 2001.

[6] A. Sinha and K. Singh, "A technique for image encryption using digital signature," Optics Communica- tions 218, pp. 229–234, 2003

[7] A. Eskicioglu and E. Delp, "An Overview of Multimedia Content Protection in Consumer Electronics Devices," Signal Processing: Image Communication 16(7), pp. 681–699, 2001.

[8] F. Y. Shih and S. Y. Wu, "Combinational image watermarking in the spatial and frequency domains," Pattern Recognition 36, pp. 969–975, 2003.

[9] X. Xu, S. Dexter, and A. Eskicioglu, "A Hybrid Scheme for Encryption and Watermarking," in Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents VI, P. Wong and E. Delp, eds., 5306, pp. 725–736, SPIE, IS&T, (San Jose, CA, USA), January 2004

[10] A. Lemma, S. Katzenbeisser, M. Celik, and M. van der Veen, "Secure Watermark Embedding through Partial Encryption," in International Workshop on Digital Watermarking (IWDW 2006), 4283, pp. 433–445, Springer Lecture Notes in Computer Science, 2006.A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII (4), pp. 605-635, 1992. (journal style)

[11] S. Lian, Z. Liu, R. Zhen, and H. Weng, "Commutative watermarking and encryption for media data," Optical Engineering 45(8), pp. 080510–1–080510–3, 2006.

[12] A. Sinha and K. Singh, "A Technique for Image Encryption Using Digital Signature," Optics Communica- tions 218, pp. 229–234, April 2003.

[13] A. Kerckhoffs, "La cryptographie militaire," Journal des sciences militaires 9, pp. 5–38, 1883.

[14] W. Puech and J. Rodrigues, "A New Crypto-Watermarking Method for Medical Images Safe Transfer," in EUSIPCO'04, Vienna, Austria, pp. 1481–1484, 2004.

[15] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology 16, pp. 354–362, Mar. 2006.

[16] D. Coltuc and J.-M. Chassery, "High Capacity Reversible Watermarking," in Proc. IEEE Int. Conf. on Image Processing, Atlanta, USA, Oct. 2006.

[17] P. Zimmermann, PGP User's Guide, MIT Press, Cambridge, 1994.

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. on Information Theory 26(6), pp. 644–654, 1976.

[19] D. Stinson, Cryptography - Theory and Practice, CRC Press, Boca Raton, Florida, USA, 1995.

[20] B. Schneier, Applied cryptography, Wiley, New-York, USA, 1995.

[21] J. Daemen and V. Rijmen, "AES Proposal: The Rijndael Block Cipher," tech. rep., Proton World Int.l, Katholieke Universiteit Leuven, ESAT-COSIC, Belgium, 2002.

[22] D. R. Stinson, Cryptography: Theory and Practice, (Discrete Mathematics and Its Applications), Chapman & Hall/CRC Press, New York, November 2005.