Publication and distribution of digital assets biology essay

Science, Biology

Internet has made the publication and distribution of digital assets much easier today as compared to a time when the medium was not so popular. Digital assets are very sensitive than physical assets; they are easy to redistribute in large numbers. The owner of digital assets faces the risk of infringement of copyright protection when someone else uses or redistributes his/her work without prior consent. The original work, in the form of text, digital images, videos and audio files, are easy to access and copy on the internet infrastructure. One of the most common practices of illegal data usage is on social networking sites where some users make unauthorized of copy somebody else's image and use it on one's own profile. Hence, ownership rights of digital assets become a crucial issue. In electronic era we are challenged to overcome this problem [1]. On the other hand, E-mailing and text messaging have become a part of easy, fast and authentic way of communication. There however remains a sense of insecurity usually imposed by eavesdropper who with ulterior motive access, monitor and misuse our private communication over public communication channel on internet. Another issue that arises is more secure safeguard mechanism for private message communication on this public after all people are communicating through internet which is a public channel. So the issue arises to develop a safeguard for our private message [2, 7]. This research work focuses on the issues of improved copyright protection digital assets and secure communication secret messages. The techniques used for image protection and information hiding areDigital Watermarking Algorithm Using Random Matrix Image (RMI) as Watermark, Text File Embedment Algorithm

Watermarking and Secret Messaging, Secret Messaging using Cryptography and Steganography.

Digital Watermarking

Digital assets are facing severe ownership issues and digital watermarking is seen as a solution to curb these unfair practices. Digital watermark is an authenticating technique of digital data with secret information that can be extracted by the receptor. The image in which this data is inserted is called ‘ host image’. The watermarking process has to be resistant against possible attacks, keeping the content of the watermark readable in order to be recognized when extracted. Features like imperceptibility and fidelity are essentials of a watermarking system however the size of the embedded watermark has to be measure since data becomes less robust as its size increases. Therefore a trade-off of these features must be considered [2, 3].

Blind Watermarking Technique

A digital watermarking technique is considered blind if it does not require original data from the owner in order to extract watermark. Watermark extraction with the help of original digital assets is classified as non-blind watermarking. The blind scheme is more useful because it does not need original data and owner of the assets does not need to transmit original image through public channel-internet [3, 9].

Imperceptible Watermark

A watermark is called imperceptible watermark if it is invisible to Human Visual System (HVS). If it is visible toa naked eye then it is considered as

perceptible. Perceptible means it is visible to humans clearly like a logo inserted into the corner screen of television channels. It is also not easy to remove good perceptible watermark from an image for an unauthorized person. An imperceptible watermark is embedded into a target image by algorithm using key. So those who don't know the key and algorithm cannot extract watermark easily. Imperceptible watermark is even difficult to detect into watermarked image [3, 4].

Private Watermark

Private watermark is a watermark detected by only authorized user. Private watermark is justified if it involves all techniques and effort to make it quite impossible for unauthorized users to extract watermark. In private watermark technique, a private key is used to embed watermark to the host image. Private Key helps to know a watermark's position(x, y) into the target image [3, 6].

Fragile Watermark

Fragility refers to capacity of embedded watermark survive in day to day usage of an image or against intention or unintentional attacks. The watermark with low capacity is known as fragile. The fragile watermark is employed to inspect any change in image [5, 6].

Copyright Protection Watermark

Digital assets are published on internet; the copyright information can be inserted as a watermark. When there is a dispute on the ownership, the watermark can provide the authentic information. The watermark for

copyright protection is used for both the owner of the digital assets and the authorized user[7].

Spatial Domain Based

In the spatial domain, we can embed a watermark in the host image by changing the intensity of the gray value of selected pixels in the host image. This method has low level of complexity in implementation. The spatial domain watermarking techniques are usually less robust against compression and noise attack [3, 8].

Least Significant Bits (LSB)

Least-significant bits substitution is generally used for embedment of watermark to the image [9, 10 and 11]. The method is easy to implement. The technique is less robust.

Steganography

On public communication channel it is necessary to send message after transforming to different form to misguide eavesdropper. The sender wants to send secret message to the recipient by changing the form. For this, various cover objects are used. The steganography is used to hide information under safeguard or cover images. To effectively projecta different object instead of the original secret message is the key objective of stenography[12, 13].

Digital Steganography

Digital steganography is a technique of hiding information within the object classified as multimedia object which may include in any combination sub

objects - audio, image, and video. The information is mainly hidden in digital images because the sizes of images are comparatively large. Now a days, steganography software uses algorithms to hide information [12].

One – Time Pad

The random private key used only once to encrypt message at source and decrypt the message at destination is known as one time pad. The advantage of this method is that no one can easily guess the algorithm even by observing series of secret messages [14, 15].

Cryptography

Cryptography is referred as secret messaging technique which encrypts plain text message at source, also known as cipher text and then decrypts the cipher text at destination [12, 13 and, 17].

Use of Private Key

The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption [16, 17].

References

W. C. H. Fung, G. Antonio, and W. Godoy, " A Review Study on Image Digital Watermarking," The Tenth International Conference on Networks- ICN, pp. 24–28, 2011. X. Wu and Zhi-Hong Guan, " A novel digital watermark algorithm based on chaotic maps," Physics Letters A, Elsevier, vol. 365, no. 5–6, pp. 403–406, Jun. 2007. D. L. Bhaskari, P. S. Avadhani, and M.

Viswanath, " A Layered Approach for Watermarking In Images Based On Huffman Coding," International Journal on Computer Science and Engineering, vol. 02, no. 02, pp. 149–154, 2010. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Second Edi. Morgan Kaufmann Publishers, Elsevier, 2008. R. L. de Queiroz, " Processing JPEG-compressed images and documents.," IEEE transactions on image processing : a publication of the IEEE Signal Processing Society, vol. 7, no. 12, pp. 1661–72, Jan. 1998. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, " A DCT-domain system for robust image watermarking," Signal Processing, vol. 66, no. 3, pp. 357–372, May 1998. D. Kirovski and F. a. P. Petitcolas, " Blind pattern matching attack on watermarking systems," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 1045–1053, Apr. 2003. D. Kundur and D. Hatzinakos, " Improved robust watermarking through attack characterization." Optics express, vol. 3, no. 12, pp. 485–90, Dec. 1998. X. Qi and J. Qi, " A robust content-based digital image watermarking scheme," Signal Processing, Elsevier, vol. 87, no. 6, pp. 1264–1280, Jun. 2007. H. Kostopoulos, S. Kandiliotis, I. Kostopoulos, and M. Xenos, " A Digital Image Watermarking Technique Using Modulated Pascal ’ S Triangles," International Conference Signal Processing, Pattern Recognition & Applications, pp. 82–86, 2003. M. A. Suhail, M. S. Obaidat, S. S. Ipson, and B. Sadoun, " A Comparative Study of Digital Watermarking In JPEG and JPEG 2000 environments," Information Sciences, Elsevier, vol. 151, pp. 93–105, May 2003. R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, " A comparative Analysis of Image Steganography", International Journal of computer Applications (0975-8887), May, 2010, Vol 2, No. 3. Bret Dunber, "

Steganographic Techniques and their use in an Open-Systems Environment", SANS Institute, 01/18/2002. D. Aucsmith, " An information-theoretic model for steganography", Proceedings of the second Intel. Workshop on Information Hiding, April, 1998, pg. 306-318. R. J. Anderson, F. A. P. Petitcolas, " On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, May, 1998, pg 474-481. Ismail Avcıbas¸, NasirMemon, and BülentSankur, " Steganalysis Using Image Quality Metrics", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 12, NO. 2, FEBRUARY 2003Cryptography and Network Security, Willian Stallings, Prentice Hall of India.

Chapter - 2: Review of Related Work

Digital Watermarking Techniques and Algorithms

V. Potdar et al. [1] has revealed in their work the relationship of steganography for secret communication and watermarking for content protection, copyright management and content authentication. The authors have discussed the existing watermarking techniques towards different domains. This paper is reviewed as survey paper on digital image watermarking. E. Hassanien et al. [2] has focused on the transform domain based watermarking techniques. The robustness of the proposed algorithm is measured and the result has indicated accepted level of protection against a set of attacks. The authors have proposed a robust image watermarking algorithm for copyright protection. The algorithm is specifically based on the DWT domain. The algorithm was dealt with the watermark embedment and detection process. The experimental results have indicated that watermark

is imperceptible and robust. Jian Liu et al. [3] have outlined the properties of digital watermarking and steganography. In this work, the authors have given fairly good description of differences between watermarking, steganography and cryptography. Researchers have tried to elaborate, how one can make communication more and more secret using cryptography. The authors have also focused steganography to extend the level of secrecy of communication higher by transforming the object to its transformed type of object - different to the object communicated in cryptography. The researchers have concluded that digital watermarking is targeted to image protection under copyright protection while steganography has importance of protection of secret message rather than in which it is embedded. The authors have also added that digital watermarking is a subset of steganography. X. Qi et al. [4] have proposed a content-based digital image-watermarking technique. This work has used error correcting codes with the spread spectrum technique to encode watermark with an objective of improve in detection accuracy. The image-content-based technique was an adaptive embedding scheme which was applied in Discrete Fourier Transform (DFT). The experimental results demonstrate the robustness of the proposed method against any combination of the geometric attacks and some of the image-processing operations such as JPEG compression, filtering, and enhancement. Wu. X et al. [5] have given an improved digital watermarking algorithm. The proposed algorithm uses two chaotic maps - one is used to encrypt the position of embedment to the host image, and second one is used to obtain the pixel bit value at that position. The watermark was classified imperceptible. S. Cheung et al. [6] have proposed

the scheme which uses intelligence user certificates. This certificate was embedded for the identity of the owner/user into the digital documents. Indeed, maintaining secrecy between owners and users was a key contribution of this work. The researchers have dealt with the protocol in order to support for intelligence applications. They have outlined an implementation of the distribution protocol and watermarking scheme used. In short, a concept of document distribution protocol has been proposed to address a problem in an intelligence distribution network so that document distribution policies can be managed. Yanqun Zhang [7], in his paper, has reviewed digital watermarking techniques to protect digital assets viz. images, videos, and audios. The characteristics - imperceptibility, security, reliability, low complexity of watermarking was included in the algorithm and the security was maintained by hiding the position of embedment. D. L. Bhaskari et al. [8] have given an innovative algorithm through which large volume of data can be embedded under spatial domain techniques. In the algorithm, data is being compressed using Huffman coding and embedded using modified auxiliary carry approach. The result of this work was visualized with regard to images having grey levels from 0-255. W. Fung et al. [9]have studied watermarking techniques based on Spatial Domain, Transform Domain. As per their review findings the use of the technique of Wavelet Transform Domain combined with Singular Value Decomposition (SVD) was an approach to improve computational performance. Still further, the use of Lifting Wavelet Transform (LWT) improves computational performance. The extension of their work indicated the use of coding and cryptography in watermarks has been viewed as the future scope. R. Aarthi

et al. [10] have given an algorithm for digital image watermarking. Here, the algorithm was developed by modifying LSB embedding strategy which covers reversibility by using two bits in every pixel for embedment. Here reversibility was viewed as major feature. Reversibility - In watermarking process after getting the watermarked image, one need to create a matrix initialized with zeros, whose dimension was equal to the watermarked image. By XOR-ing each pixel of both the original and watermarked image, one can created new matrix. The matrix will also be sent to the extraction phase to the authorized person. In extraction process the value of the newly created matrix will be checked. If it is 1, then watermarked image's s LSB of each pixel must be changed, else vice versa. By this one could get back the original image. The algorithm which provides reversibility is motivational digital image watermarking.

Integration of Cryptography and Steganography for Information Hiding

M. S. Prasad et al. [11] have proposed, in this paper, a method to provide security for the key information by integrating image compression and data encryption method. Quantization compression technique was applied for the file contains lots of repetitive data. Gary C. Kessler [12] has summarized technical introduction of steganography. This is reviewed as a descriptive historical research in context of steganography. The research work has suggested digital applications for hiding information in online image or audio files. M. K. Sharma et al. [13] have derived comparative study of steganography and watermarking. The different parameters were defined. Finding of this paper has suggested how these techniques can be integrated

as an extension in the field where security of digital assets and data plays the major role. M. Gokul et al. [14] have given, in this paper, a hybrid watermarking technique to embed a secret message into an image using visual cryptography and SLSB(Selected Least Significant Bit) encryption techniques. The work can be extended by applying a DCT based compression on the secret image for further security and the LSB bit encryption algorithm can be changed with a more complicated method. J. Nath et al. [15] have given method for hiding any secret message by embedding it into an image. The randomization method for generating the key matrix to encrypt plain text file at source and to decrypt cipher text file at destination was used. The maximum length of the key was 16 characters long and contains any character. The size of the encryption key matrix was of 16 X 16. As an extension of this work, security can be increased by increasing size of matrix. T. Chatterjee at al. [16] has presented a method in which modified a cipher method using XOR operation was used. The overhead of the present method was very less. This method was applied specially in encryption of data where the same pattern is repeated or to encrypt short message or password. Use of different key matrix by extending size is an extension of this work. S. Dey et al. [17] have proposed algorithm named as SJA-I (Somdip Joyshree Asoke). This algorithm was applied to encrypt short length text message. SJA-1 was the integration of different algorithms: Each byte is converted into its corresponding binary number and then after single bit operation was executed on that, Secondly, the use of modified Caesar Cipher algorithm was applied on the message randomly. Another technique of cryptography can be a research extension.

Literature Review Analysis and Findings

The literature review of digital watermarking, initially, suggests an extension of work to develop unique imperceptible watermark [2, 5, and 7]. Secondly, the use of encryption method should be applied before embedding message to digital image [8]. The use of random key matrix for embedment and extraction is also suggested [10, 15-17]. The use of symmetric key and one time pad method has also played significant role in the work for encryption and decryption [16, 17].

Problem Statement

The challenge regarding significant characteristics of digital watermark - uniqueness, imperceptibility and reversibility is undertaken as a research problem. The blind watermarking scheme is used as a key technique to strengthen the protection issue as the original image is never require to communicated at the destination. The targeted research work is intended to evolve out an algorithm, which can be used for both copyright protection of an image and secret messaging for communication. The issue secrecy enhancement is undertaken to extend the work [10, 15 and 16] with a focus on watermark embedment and secret message embedment techniques using encryption with an intention to increase the level of secrecy and imperceptibility without increasing the level complexity of algorithm.

References

V. M. Potdar, S. Han, and E. Chang, " A survey of digital image watermarking techniques," 3rd IEEE International Conference on Industrial Informatics, 2005. India, pp. 709–716, 2005. E. Hassanien, " A Copyright Protection using

Watermarking," INFORMATICA, Institute of Mathematics and Informatics, Vilnius, vol. 17, no. 2, pp. 187–198, 2006. Jian Liu and Xiangjian He, " A Review Study on Digital Watermarking", Department of Computer Systems University of Technology, Sydney. 2007X. Qi and J. Qi, " A Robust Content-Based Digital Image Watermarking Scheme," Signal Processing, ELSEVIER, vol. 87, no. 6, pp. 1264–1280, 2006. Wu, X., & Guan, Z.-H. (2007). " A Novel Digital Watermark Algorithm Based on Chaotic Maps". Physics Letters A, ELSEVIER, 365(5-6), 403–406. doi: 10. 1016/j. physleta. 2007. 01. 034S.-C. Cheung, D. K. W. Chiu, and C. Ho, " The Use of Digital Watermarking for Intelligence Multimedia Document Distribution," Journal of Theoretical and Applied Electronic Commerce Research, vol. 3, no. 3, pp. 103–118, Dec. 2008. Yanqun Zhang. " Digital Watermarking Technology: A Review", Conference Publications, IEEE Explore, 2009D. L. Bhaskari1, P. S. Avadhani, and M. Viswanath, " A Layered Approach for Watermarking In Images Based On Huffman Coding," International Journal on Computer Science and Engineering, vol. 02, no. 02, pp. 149–154, 2010. W. C. H. Fung, G. Antonio, and W. Godoy, " A Review Study on Image Digital Watermarking", The Tenth International Conference on Networks- ICN, pp. 24–28, 2011. R. Aarthi, V. Jaganya, and S. Poonkuntran, " Modified LSB Watermarking for Image Authentication," International Journal of Computer & Communication Technology (IJCCT), vol. 3, no. 3, pp. 62–65, 2012. M. S. Prasad, S. Naganjaneyulu, and C. Nagaraju, " A Novel Information Hiding Technique for Security by Using Image Steganography", Journal of Theoretical and Applied Information Technology (JATIT), 2009. G. C. Kessler, " An Overview of Steganography for the Computer Forensics Examiner," Forensic Science

Communications, pp. 1–29, 2011. M. K. Sharma and P. Gupta, " A Comparative Study of Steganography and Watermarking," IJRIM, vol. 2, no. 2, pp. 1–12, 2012. M. Gokul and R. Umeshbabu, " Hybrid Steganography using Visual Cryptography and LSB Encryption Method," International Journal of Computer Applications, vol. 59, no. 14, pp. 5–8, 2012. J. Nath and A. Nath, " Advanced Steganography Algorithm using Encrypted secret message," International Journal of Advanced Computer Science and Applications,, vol. 2, no. 3, pp. 19–24, 2011. T. Chatterjee, T. Das, S. Dey, J. Nath, and A. Nath, " Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method : TTSJA algorithm," International Journal of Computer Applications, vol. 42, no. 1, pp. 34–39, 2012. S. Dey, J. Nath, and A. Nath, " An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation , Bit Reversal , Modified Caesar Cipher (SD-REE), DJSA method , TTJSA method : SJA-I Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012. International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012.

Chapter - 3: Proposed Work

The proposed work includes three algorithms. The first one is used to provide protection to an image with reference to copyright protection by embedding Random Matrix Image (RMI) as watermark which indicates use of random key [1, 2 and 3]. Second algorithm embeds text watermark, which is used for secret messaging also. This research workaims togo further by usinga third technique that involves cryptography, steganography and watermarking

techniques on spatial domain. The work is extended by integrating these techniques using symmetric key and one time pad. The proposed work is implemented under SCILAB environment.

Watermarking Algorithm using RMI as Watermark

Digital Watermarking Process

A digital image watermarking process includes three phases, first embedment, second detection and third extraction. In embedment, an algorithm takes an image as it an original image and then watermarks that image or data [1]. The watermarked image is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack [2, 8]. There are various kinds of attacks like copy, removal, mosaic etc. Watermark detection is an algorithm which is used to find the attacked data to attempt to extract the watermark from it. If the watermarked image is not modified during transmission, then the watermark is still present and it can be extracted. If the watermarked image is copied, then the information is also carried in the copy. The embedment uses a place by manipulating the content of the digital assets, which means the information is not embedded in the frame around the data, but it is carried with the watermarked image itself [3, 10]. In figure 1 watermark embedment process is shown and in figure 2 watermark extraction processes is shown.

Original Image

(O)

)

Original Watermark

(W)

Embedment

WI= O+W

Watermarked Image

(WI)

Using KeyFIGURE 1: WATERMARK EMBEDMENT PROCESS

Original Image

(O)

)

Original Watermark

(W)

Extraction

O= WI–W

Watermarked Image

(WI)

Using KeyFIGURE 2: WATERMARK EXTRACTION PROCESSDigital watermark is an authenticating technique of digital data with secret information that can be extracted to the receptor. The image in which this data is inserted is

called ‘ cover image’ or ‘ host image [4]. The watermarking process has to be resistant against possible attacks, keeping the content of the watermark readable in order to be recognized when extracted. Features like robustness and fidelity are essentials of a watermarking system. However the size of the embedded information has to be considered since data becomes less robust as its size increases. Therefore a trade-off of these features must be considered [5, 7 and 11]. In the algorithm, the focus is on the development of improved technique to generate unique watermark and embed watermark to host image. The targeted output is in form of watermarked image. In this work Random Matrix Image (RMI) is generated and embedded as a watermark. A watermark is generated as a unique RMI for each host image for watermarking. The proposed algorithms are used for watermark generation, embedment, and extraction in watermarking. The exact reverse process is used toextract watermark form watermarked image [9]. For extraction, it is required to use RMI key matrix or an original image.

Random Matrix Image (RMI).

RMI is an output of matrix generation process, created using randomly selected number. The random number generator is defined by the follows: X_{n+1} equiv left(a X_n + c ight)~~pmod{m}HereX is the sequence of pseudorandom values, andm,, 0 6

7

6

9

2

7

8

5

3

9

5

1

0

9

3

1

7

2

8

5

8

2

4

10

5

4

8

4

1

6

4

2

3

10

10

0

9

3

7

0

7

5

8

5

0

4

8

8

1

5

4

8

2

9

4

1

4

6

2

6

5

8

8

10

FIGURE 3: 8X8 MATRIX OF RMI

Watermark Embedment Algorithm

Step1: Read the original image. Step2: Generate RMI (having pixels values from 0 to 10) which is to be embedded as watermark. (also sent to recipient as a Secret Key Matrix)Step3: Add this Generated Image and Original Image in matrix addition form. Step4: Now generate image from matrix form. Step5: The output image is a watermarked image.

Watermark Extraction Algorithm

Step1: Read the watermarked image. Step2: Read matrix (a secret key RM) which is sent. Step3: Subtract Matrix from watermarked Image in matrix subtraction form. Step4: Now generate two different images from these matrices form. Step5: The output images will be Original image and original watermarked.

Text File Embedment Technique for Watermarking and Secret Massaging

Steganography deals with the writing of hidden messages into target object [6]. It means " concealed writing". It manages security through obscurity. Cryptography deals with encryption of target object. The target object after encryption gets transformed form readable state to non-readable (non-sense) state. Digital watermarking embeds digital watermark to target object in order to trace copyright infringements and to verify the authenticity. Digital watermarking is for source tracking. Both steganography and digital watermarking relate to information hiding with different purposes and employ Steganographic techniques to embed data [12, 18 and 19]. Steganography methods usually do not need to provide strong security

against removing or modification of the hidden message. Watermarking methods need to be very robust to attempt to remove or modify a hidden message. [13, 14]FIGURE 4: GENERIC PROCESS OF DIGITAL IMAGE WATERMARKINGAND STEGANOGRAPHYThis work aims at developing embedding algorithm where by text files in ASCII format with image file in binary format is used to generate composite file in image format. The algorithm hides the secret message in the image. The same algorithm embeds digital watermark in text format to the image. The output of this algorithm will be communicated to the recipient. The recipient with objective of extracting hidden message will separate the image and the secret message by developed extraction algorithm. The same algorithm will help to ascertain the originality of an image by extracting watermark from the image. [15, 16]The proposed algorithm is used to embed the text to the grayscale digital image without any change in intensity of grayscale level of the image. After this process the matrix tables of original image and the image generated after the embedment matched with each other. The developed algorithm does not encrypt text, as a result at the recipient end; text (secret message) can be extracted without any key. [17, 19]

Text File Embedment Algorithm

Step 1: Read the original image. Step 2: Read the text file. Step 3: Embed text file with image by inserting image file by treating image file in form of binary file. Step 4: Write/produce stego/watermarked image. Step 5: The output image is a stego/watermarked image.

Text Extraction Algorithm

Step 1: Read the stego/watermarked image in binary form. Step 2: Find Delimiters from a stego/watermarked image. Step 3: Extract characters starting from delimiters to ending delimiters. Step 4: Store extracted text in another text file.

A Secret Messaging and Watermarking Algorithm using Cryptography

Though success to certain extent has been achieved more robust work is needed for hiding secret messages from eavesdroppers. Steganography and Cryptography in combination comes for this help [18, 19]. The secret message which is to be communicated is in its hidden state so that it does not come to the notice of eavesdropper [6, 20, and 21]. Under the banner of cryptography the secret message is first encrypted with a key and then this encrypted message is sent to destination. The key is also to be sent hidden. This poses two fold challenges because at the destination the encrypted message should be received and it is to be decrypted with key. The approach that can be adopted is that the encrypted message can be embedded to target image and embedded image is then sent to target. This gives a feel of image communication rather than secret message communication, this falls under the banner of Steganography. Here too there is a challenge of sending encryption key and embedment key. In case of embedment key there are two options – static key or dynamic key. The dynamic key provides more robust secrecy compare to static key [19, 20 and 22]. Use of dynamic key is adopted in this work and to improve secrecy of message. The use of symmetric cryptography is considered with encryption and decryption using

same key. [23] Further, the key used in symmetric cryptography is also used in embedment of encrypted message to the digital image. This kind of work is not traced in literature survey. The single key which is used for encryption at source, decryption at destination and embedment at source and extraction at destination serves the purpose of secrecy maintenance. The management of key is easy but at the first sight it appears to be " the secrecy of the key is a crucial issue". In the adopted approach the disclosure of key does not give the decryption and extraction easily because the key is same in both the process but the algorithm are different and not known to eavesdropper [24]. The key is communicated through secure channel. At destination end the algorithm which extracts the encrypted secret message. After the extraction isdone the same key will be utilized for decryption of separated encrypted message to get the secret message in its original form. Encryption key is in the form of text which is decided on the basis of size of text message. The proposed algorithm does not permit repetition of character in key [18, 29]. Proposed algorithm AMEADT used to encrypt and decrypt secret message. This algorithm is based on ASCII value of a secret key[26]. Another algorithm AMEAET is used to embed and extract secret message from digital image. This is using ASCII value to decide the position of embedment in image pixel matrix. This technique follows the method of cryptography to encrypt and decrypt text message using ASCII value of a Key. Here key is dynamic so protection is high. The process of encryption is as follows [25, 28]. Here, we have a key " MESAGT" and all experiments have been done based on this key.

ASCII Message Encryptions and Decryptions Technique (AMEADT)

Step1: Find the ASCII value of Private Key as shows in Table-1TABLE 1: PK AND ASCII VALUE OF PK

PK Text

ASCII value

M77E69S83A65G71T84Step2: Sort them in ascending order as shows in Table-2TABLE 2: SORTED FORM OF PK

PK Text

ASCII value

A65E69G71M77S83T84Step3: Find the ASCII value of " Original Secret Message". Here secret message is " SECRET" as shows in Table 3TABLE 3: SECRET TEXT AND ITS ASCII VALUE

Message

Text

ASCII Value of

Secret Text

S83E69C67R82E69T84Step4Add Sorted form of ASCII value of Key into Original Secret Message for Encryption as shown in Table 4TABLE 4: ENCRYPTED TABLE FOR GIVEN EXAMPLE

PK in

Ascending

order

ASCII of PK

OSM

ASCII

of OSM

Encrypted

Value

A65S83148E69E69138G71C67138M77R82159S83E69152T84T84168Encrypted value, shown in Table 4, is embedding to digital image using AMEAET. To decrypt at destination reverse process is used.

ASCII Message Embedment and ExtractionTechnique (AMEAET)

Step1Select the image matrixpositions as shown in figure 5 according to ASCII value in ascending order. Here code is {65, 69, 71, 77, 83, and 84}So value is placed at{(6, 5), (6, 9), (7, 1), (7, 7), (8, 3), and (8, 4)}12345678912345678FIGURE 5: EMBEDMENT POSITIONS ACCORDING TOASCII VALUEOF PKStep2The encrypted message is embedded at selected position as shown in figure 5is to be changed with Encrypted Value Show in Table 3. The output result is shown in Figure 6123456789123456148138713815981521 68FIGURE 6: EMBEDMENTOF ENCRYPTED VALUEACCORDING TOASCII VALUE OF PK. Stego-image [31] is

obtained as result of this process. The reverse process of embedment gives steps of extraction process. After extraction of encrypted value the reverse steps of encryption process is used to decrypt the secret message. The decryption process after extraction phase is shown in table 5. TABLE 5: DECRYPTION TABLE

PK in Ascending order

ASCII of PK

Stego image (x, y)

Extracted – PK

Decrypted Value

SM

A65(6, 5)148-6583SE69(6, 9)138-6969EG71(7, 1)138-7167CM77(7, 7)159-7782RS83(8, 3)152-8369ET84(8, 4)168-8484TSame algorithm can be applied for watermarking also. This will give you one level high security to image.

References

W. C. H. Fung, G. Antonio, and W. Godoy, " A Review Study on Image Digital Watermarking," The Tenth International Conference on Networks- ICN, pp. 24–28, 2011. X. Wu and Zhi-Hong Guan, " A novel digital watermark

algorithm based on chaotic maps," Physics Letters A, Elsevier, vol. 365, no. 5–6, pp. 403–406, Jun. 2007. Raman, S. (2010). Image Processing Using Scilab, 1–29. Galda, H. (2011). Image Processing with Scilab and Image Processing Design Toolbox. D. L. Bhaskari, P. S. Avadhani, and M. Viswanath, " A Layered Approach for Watermarking In Images Based On Huffman Coding," International Journal on Computer Science and Engineering, vol. 02, no. 02, pp. 149–154, 2010. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Second Edi. Morgan Kaufmann Publishers, Elsevier, 2008. R. L. de Queiroz, " Processing JPEG-compressed images and documents.," IEEE transactions on image processing : a publication of the IEEE Signal Processing Society, vol. 7, no. 12, pp. 1661–72, Jan. 1998. D. Kundur and D. Hatzinakos, " Improved robust watermarking through attack characterization." Optics express, vol. 3, no. 12, pp. 485–90, Dec. 1998. X. Qi and J. Qi, " A robust content-based digital image watermarking scheme," Signal Processing, Elsevier, vol. 87, no. 6, pp. 1264–1280, Jun. 2007. H. Kostopoulos, S. Kandiliotis, I. Kostopoulos, and M. Xenos, " A Digital Image Watermarking Technique Using Modulated Pascal ’ S Triangles," International Conference Signal Processing, Pattern Recognition & Applications, pp. 82–86, 2003. M. A. Suhail, M. S. Obaidat, S. S. Ipson, and B. Sadoun, " A comparative study of digital watermarking in JPEG and JPEG 2000 environments," Information Sciences, Elsevier, vol. 151, pp. 93–105, May 2003. M. SreeramaMurty, D. Veeraiah, and a Srinivas Rao, " Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis," Signal & Image Processing : An International Journal, vol. 2, no. 2, pp. 170–179, Jun. 2011. R. Amirtharajan, R. Akila, P.

Deepikachowdavarapu, " A comparative Analysis of Image Steganography", International Journal of computer Applications (0975-8887), May, 2010, Vol 2, No. 3Bret Dunber, " Steganographic Techniques and their use in an Open-Systems Environment", SANS Institute, 01/18/2002. D. Aucsmith, " An information-theoretic model for steganography", Proceedings of the second Intel. Workshop on Information Hiding, April, 1998, pg. 306-318. R. J. Anderson, F. A. P. Petitcolas, " On the Limits of Steganography", IEEE Journal ofhttp://www. fi. muni. cz/ Definition of Steganography [ppt CHAPTER 13 - Steganography and Watermarking]D. Kirovski and F. a. P. Petitcolas, " Blind pattern matching attack on watermarking systems," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 1045–1053, Apr. 2003. R. Aarthi, V. Jaganya, and S. Poonkuntran, " Modified LSB Watermarking for Image Authentication," International Journal of Computer & Communication Technology (IJCCT), vol. 3, no. 3, pp. 62–65, 2012. J. Nath and A. Nath, " Advanced Steganography Algorithm using Encrypted secret message," International Journal of Advanced Computer Science and Applications,, vol. 2, no. 3, pp. 19–24, 2011. S. Dey, J. Nath, and A. Nath, " An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation , Bit Reversal , Modified Caesar Cipher (SD-REE), DJSA method TTJSA method : SJA-I Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012. International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012. A. Nath, S. Ghosh, M. A. Mallik, " Symmetric Key Cryptography using Random Key generator:" Proceedings of International conference on security and management(SAM2010) held at Las Vegas, USA Jully 12-15, 2010), P-Vol-2,

239-244 (2010). D. Chatterjee, J. Nath, S. Mondal, S. eepDa. key Cryptography using extended MSA method: DJSSA symmetric key algorithm" Jounal of Computing, Vol3, issue-2, Page 66-71, Feb(2011). J. Nath and A. Nath, " Advanced Steganography Algorithm using encrypted secret message" International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March(2011). D. Chatterjee, J. Nath, S. Dasgupta and A. Nath, " A new Symmetric key Cryptography Algorithm using extended MSA method : DJSA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June, 2011, Page-89-94. N. Khanna, J. James, J. Nath, S. Chakraborty, A. Chakrabarti and A. Nath " New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm" Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 03-06 June 2011, Page 125-130. D. Das, J. Nath, M. Mukherjee, N. Chaudhury and A. Nath, " An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE conference WICT-2011 held at Mumbai University Dec 11-14, 2011D. Chatterjee, J. Nath, S. Das, S. Agarwal and A. Nath, " Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at Las Vegas, USA, July 18-21, Page 312-318, Vol-I(2011). J. Nath. et. al. " Symmetric key Cryptography using two-way updated -Generalized Vernam Cipher method: TTSJA algorithm" IJCA, Volume 42– No. 1, March 2012Cryptography and Network Security, Willian Stallings, Prentice Hall of India.

Chapter - 4: Implementation and Results

Watermarking Algorithm using RMI as Watermark

Experiment using 256 X 256 Size Grayscale Image

Watermarking algorithm using RMI as watermark was experimented using various sizes of grayscale images. Here, the result of " Lena" image with 256 × 256 pixel size and 256 × 256 pixel size watermark (RMI) is shown. Figure 7(a) and 7(b) shows greyscale image of 256X256 pixel size Lena image and generated RMI watermark respectively. Figure 8(a) and 8(b) show 8X8 pixel size matrix of Figure 7(a) and 7(b) images respectively and figure 9(a) and 9(b) shows watermarked image and 8x8 matrix of watermarked Lena image.

(a)

(b)

FIGURE 7: (a) ORIGINAL LENA IMAGE (b) RMI WATERMARK195195196197197198199199196196196197197198198197197197197196196196199198198197196195194194199198197196195194193193198198197196195194193193197196196195195194194196196195195194194194

(a)

229826367200008391304011263072429306367255377052510758052055976 6

(b)

FIGURE 8:(a) 8X8 MATRIX OF LENA IMAGE(b) 8X8 MATRIX OF RMI WATERMARK

(a)

19719720520519920420220520319819619719719720620120619820019720019619719720120420119720319719819620820119720219820020019520320320020320219419819520219719620220020219419919819620020020420120020 0

(b)

FIGURE 9:(a) WATERMARKED LENA IMAGE

(b) 8X8 MATRIX OF WATERMARKED IMAGE

In the experiment the result shown in figure 9(b) is the addition of two matrices shown in figure 8(a) and figure 8(b). The changes in intensity of grayscale values are not reflected the watermarked to Lena image. This show that watermark is imperceptible [1, 2].

Experiment using 512 X 512 size grayscale image.

The result of various sizes of images was examined and another one of them is presented here. The work is shown is of 512 X 512 size grayscale image. Figure 10(a) and 10(b) shows greyscale image of 512X512 pixel size peepers image and generated RMI watermark respectively. Figure 11(a) and 11(b) show 8X8 pixel size matrix of figure 10(a) and 10(b) images respectively and figure 12(a) and 12(b) shows watermarked peepers image and 8x8 matrix of watermarked peppers image.

(a)

(b)

FIGURE 10: (a) ORIGINAL PEPPERS IMAGE (b) RMI

WATERMARK3758636166595257381161141161121141121063812411611111211111210840111120106119110106106371121251171101201081124211012310710910711611238110104114104116111110391091171021121111121102

(a)

2

0

5

9

0

9

6

1

7

4

7

8

4

8

8

4

1

7

6

9

6

6

1

9

9

9

6

0

1

9

5

7

7

9

8

6

1

5

6

6

8

7

4

8

9

7

2

4

6

8

9

8

5

1

5

7

6

2

2

7

6

9

7

9

(b)

FIGURE 11: (a) 8X8 MATRIX OF PEPPERS IMAGE(b) 8X8 MATRIX OF RMI WATERMARK

(a)

39

58

68

70

66

68

58

58

45

120

121

124

116

122

120

110

39

131

122

120

118

117

113

117

49

120

126

106

120

119

111

113

44

121

133

123

111

125

114

118

50

117

127

115

118

114

118

116

44

118

113

122

109

117

116

117

45

111

119

109

118

120

119

111

(b)

FIGURE 12:(a) WATERMARKED PEPPERS IMAGE(b) 8X8 MATRIX OF WATERMARKED IMAGEThe analysis of figure 12(b) shows the addition of two matrices as shown in image figure 11 (a) and 11(b) as it was happened in previous Lena image. The change in grayscale intensity [3] is not reflected after embedment of RMI watermark to peppers shown in figure 12(a).

Text File Embedment Technique for Watermarking and Secret Massaging

Experiment of algorithm described in chapter 3. 2 is done by using 64X64 pixel peeper image. Figure 13(a) shows grayscale image of 64X64 pixels and Figure 13(b) shows 8X8 pixel matrix of peeper. Figure 14 is a text file of message which is used to be embedded. And Figure 15 (p) shows output image and 15(q) 8x8 matrix of peepers image [3, 4]. peppers256

(a)

67818480528290756910710010912010396106110162155165179138103961371891951981921811006912718918919420220977921372091871942201895314113719819119819112283159981391771871296214315 3

(b)

FIGURE 13:(a) GRAYSCALE " PEEPERS" IMAGE OF 64X64 PIXEL(b) 8X8 MATRIX OF PEEPERSFIGURE 14: TEXT FILE OF SECRET MESSAGE / LICENSING INFORMATIONpeppers256

(p)

678184805282907569107100109120103961061101621551651791381039613718919519819218110069127189189194202209779213720918719422018953141137198191198191122831599813917718712962143153

(q)

FIGURE 15:(p) WATERMARKED " PEEPERS" IMAGE OF 64X64 PIXEL(q)8X8 MATRIX OF WATERMARKED " PEEPERS" IMAGEThe proposed algorithm is also experimented using 256X256 pixel grayscale ipexcell image. Figure 16(a) shows grayscale image of 256X256 pixels and 16(b) shows 8X8 pixel matrix of ipexcell. Figure 17 is a text file of message which is used to be embedded. And figure 18 (p) shows output image and 18(q) 8x8 matrix of watermarked ipexcell image. The image is taken as to experiment is with reference previous work done by R. Aarthi et al.[4]

cell

(a)

119115112112112115124133118114112112110114131150117113112112108113141173117112111111107116152190115112110109111128163196112112108108122149177194108111107108135174193191105110106109144191204189

(b)

FIGURE 16:(a)GRAYSCALE " IPEXCELL" IMAGE OF 256X256 PIXELS(b) 8X8 MATRIX OF " IPEXCELL" FIGURE 17: TEXT FILE OF SECRET MESSAGE/LICENSING INFORMATION. cell

(p)

119115112112112115124133118114112112110114131150117113112112108113141173117112111111107116152190115112110109111281631961121121081081221491771941081111071081351741931911051101061091441912041 89

(q)

FIGURE 18:(p) WATERMARKED " IPEXCELL" IMAGE OF 256X256 PIXELS(q) 8X8 MATRIX OF WATERMARKED " IPEXCELL" Figure 15 (p) shows that watermarked Peeper image and 15(q) shows 8X8 matrix of peeperswatermarked image. The same way Figure 18(p) shows that watermarked " ipxcell" image, 18(q) shows 8X8 matrix of ipexcell watermarked image. This categorically indicates that there is no change in the matrices as well as in images.

A Secret Messaging and Watermarking Algorithm using Cryptography

The proposed algorithm is checked using grayscale images of various sizes having resolution > 256 x 256 are used. Here " Barbara. jpg" and " boat. jpg" images are shown. Plain text= " SECRET", PK = MESAGTEncrypted Value is: {148, 138, 138, 159, 152, 168}Embedment Position is shown in Figure 20(b) (using PK). G: imagesarbara. jpg1802002051921901931962062121751972011891901931962072141731951941831881931982102111832001931811871932002132121972081941841901942012122081992031901871941962042112021951931831881971991

208211199195190180190199201211212186202192189195204207214208177

(a)

(b)

FIGURE 19:(a) BARBARA COVER IMAGE OF 512X512 PIXELS(b) 9X9 PIXEL MATRIX OF BARBARA COVER IMAGEG: imagesarbara. jpg

(b)

180200205192190193196206212175197201189190193196207214173195194183188193198210211183200193181187193200213212197208194184190194201222081992031901871481962042111381381931831881971991592111991951901521681992012112121862021921891952042072142081

(b)

FIGURE 20:(a) BARBARA STEGO IMAGE OF 512X512 PIXELS(b) 9X9 PIXEL MATRIX OF STEGO IMAGEG: imagesoat. jpg

(a)

128123126117127124125129126129126128123125124124129126127126128127123126126130129125124128128123126128129130126126128127124125129126129126127127125126126130126130124130124125124127129127130124134123125121126124125127126127126127126124126132127

(b)

FIGURE 21:(a) BOAT COVER IMAGE OF 512X512 PIXELS.(b) 9X9 PIXEL MATRIX OF BOAT COVER IMAGEG: imagesoat. jpg

(a)

128123126117127124125129126129126128123125124124129126127126128127123126126130129125124128128123126128129130126126128127124125129126129126127127125148126130126138138130124125124127159127130124134152168121126124125127126127126127126124126132127

(b)

FIGURE 22:(a) BOAT STEGO IMAGE OF 512X512 PIXELS.(b) 9X9 PIXEL MATRIX OF STEGO IMAGEThe stego-image/watermarked image is the output of the given encryption and embedment algorithm [5, 6 and 7]. Here, the result shows that after embedding the secret message / watermark text according to PK to the Stego image [8] of Barbara shown in figure 20(a) and the stego image of Boat shown in figure 22(a) seems no change in comparison of original imageof Barbara shown in figure 19(a) and original image of boat image shown in figure 21(a) respectively. They are changed but the changes are not detected by Human Visual System (HVS)[9, 10]. The changes is visualized by observing the matrices of stego Barbara image shown in figure 20(b) and matrix of stego boat image shown in figure 22(b) comparing with matrix of original Barbara image shown in figure 19(b) and matrix of original boat image shown in figure 21(b) respectively. Theseimages and all other images of different size is experienced this. But there is a need to remember that message size and key size must be less than 255 characters. The algorithms are applied in reverse order at destination. Only authorized person can do this. This means the person (user) having PK can extract

encrypted message/watermark and decrypt message/watermark. The example of decryption process is shown in Table 5.

TABLE 6: DECRYPTION TABLE FOR CURRENT PK

PK in

Ascending

order

ASCII of

Key

stego image

(x, y)

Extracted – PK Value

Decrypted Value

SM

A65(6, 5)148-6583SE69(6, 9)138-6969EG71(7, 1)138-7167CM77(7, 7)159-7782RS83(8, 3)152-8369ET84(8, 4)168-8484T

References

D. L. Bhaskari, P. S. Avadhani, and M. Viswanath, " A Layered Approach for Watermarking In Images Based On Huffman Coding," International Journal on Computer Science and Engineering, vol. 02, no. 02, pp. 149–154, 2010. Raman, S. (2010). Image Processing Using Scilab, 1–29. Galda, H. (2011). Image Processing with Scilab and Image Processing Design Toolbox. R. Aarthi, V. Jaganya, and S. Poonkuntran, " Modified LSB Watermarking for

Image Authentication," International Journal of Computer & Communication Technology (IJCCT), vol. 3, no. 3, pp. 62–65, 2012. J. Nath and A. Nath, " Advanced Steganography Algorithm using Encrypted secret message," International Journal of Advanced Computer Science and Applications,, vol. 2, no. 3, pp. 19–24, 2011. S. Dey, J. Nath, and A. Nath, " An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation , Bit Reversal , Modified Caesar Cipher (SD-REE), DJSA method TTJSA method : SJA-I Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012. International Journal of Computer Applications (0975 – 8887), vol. 46, no. 20, pp. 46–53, 2012. Nath, S. Ghosh, M. A. Mallik, " Symmetric Key Cryptography using Random Key generator:" Proceedings of International conference on security and management(SAM2010) held at Las Vegas, USA Jully 12-15, 2010), P-Vol-2, 239-244 (2010). D. Chatterjee, J. Nath, S. Mondal, S. eepDa. key Cryptography using extended MSA method: DJSSA symmetric key algorithm" Jounal of Computing, Vol3, issue-2, Page 66-71, Feb(2011). J. Nath and A. Nath, " Advanced Steganography Algorithm using encrypted secret message" International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March(2011). D. Chatterjee, J. Nath, S. Dasgupta and A. Nath, " A new Symmetric key Cryptography Algorithm using extended MSA method : DJSA symmetric key algorithm", Proceedings of IEEE CSNT-2011 held at SMVDU(Jammu) 3-5 June, 2011, Page-89-94.

Chapter-5: Conclusion and Extension of Work

Conclusion

Watermarking Algorithm using RMI as Watermark

A novel method of digital watermarking based on embedding matrix as a watermark is presented in this work. This uses random matrix as a watermark to protect digital images. The motive for this is that each image usually has different matrix from 0 to 10. The noticeable part of this work is the use of RMI transition to authenticated user of the image. Without having RMI, no one other than the authenticated user can detect and extract watermark from a watermarked image. The limitation of the current work is that the stated technique of digital water marking is used on grey scale image [1] and not on the coloured image. The test is performed on greyscale image having less than 245 greyscale pixel value.

Text File Embedment Technique for Watermarking and Secret Massaging

This technique shows the text message embedment to image and extraction of text message algorithms. These algorithms particularly in embedment algorithm embeds text message to an image without changing pixel value of the original image which does not give any clue of embedment of additional object into the image. However, the additional object is embedded without changing its properties. The extraction algorithm is also simple whereby it extracts the additional object (in this case text message from the image). The technique can further be imprive by changing the property of the text message embedded into several images in diversified ways. In future we

may embed encrypted text file to image to provide more secure communication and watermark. Thelimitationof the algorithm is that a removal attack can destroy the message text as it is a fragile watermark [2].

A Secret Messaging and Watermarking Algorithm using Cryptography

The third algorithm proposes a technique which increases the level of secrecy in communication [3]. This improvement in secrecy level is achieved by combining the techniques: AMEADT and AMEAET using single key for both encryption/decryption and embedment/extraction. In the earlier works researchers [2] focused on improving the complexity of encryption and using static technique of embedment. Our approach does take special care of the security level in the embedment phase. The increasing complexity in any technique may increase the level of security but at the cost of processing time. The proposed work takes special care to increase the level of secrecy in encryption by user defined dynamic key, without increasing the complexity of algorithm. This reduced complexity is extended to use of the same dynamitic key for embedment. This leads to the enhancement of secrecy level. This research work has a limitation with regard to the size message and the key to be communicated has to be less than 255 characters in size. This indicated limitation on message size is not limitation if a long message is communicated fragmenting it in sub-messages and then integrating them at destination., this not only eliminate the stated limitation in case of size of manage but also enhanced level of secrecy. The proposed work using a message having limitation of maximum 255 characters requires image object for embedment to have a minimum resolution size of 256x256

pixels. If the image size is larger than the message size then the encrypted data in the image is imperceptible. This also reduces the apparent doubt of any embedment.

Future Extension

The extension of this work can cover the use of stated technique of digital water marking on colour images. The research extension directs scheme watermarking with use of segmentation base watermarking.