SECURE PIXEL-WISE EMBEDDING METHOD FOR IMAGE WATERMARKING TECHNIQUE

Sreeparna Chakrabarti
Research Scholar, Visvesvaraya Technological University, Belagavi, India.

Dr. G.N.K. Suresh Babu
Professor, Department of Computer Applications, Acharya Institute of Technology, Bangalore, India.

ABSTRACT

Security is turning into an imperative part of life. Digital watermarking is one of the foreseen approaches to evade copyright assurance issues of multimedia information. The benefit of this procedure is that it is more affordable than other comparative strategies for information covering like digital signatures. In this paper cryptography based digital image watermarking algorithm is discussed to increase security of watermark data that can embed more number of watermarks and increase the security of watermarks. Better quality images can be given as input which will improve its performance of Mean Square Error and Peak signal noise ratio.

Keywords: Pixel wise embedding, Extraction, detection.

INTRODUCTION

Present age is observer of headways of digital media. A typical occurrence of digital media is a photo taken by cell phone camera. The use of digital media is customary these days. Some more precedents of digital media are content, sound, video and so forth. Web is the fastest medium of sending information to wherever over the globe. As these instruments are propelling, the threat of theft and copyright issues attacks each datum proprietor's mind. Thus, "watermarking" is a training embraced to shield information from these feelings of trepidation, in which holder certifications (watermark) is intertwined with the digital media at the sender's stop and at the beneficiary's end this proprietor ID is utilized to perceive the verification of information.

Since this procedure can be connected to all multimedia assortments like picture, acoustic, video and reports, for quite a while specialists and designers contemplated and worked upon here to increase best yields [1].

In the wellbeing zone, a dependable administration is unequivocally characterized as one, which ensures that the sent and got information are unclear. This twofold definition is additionally appropriate to pictures. All things considered, circumstances, pictures can be changed, their pixel esteems can be altered yet not the real significance of the picture. [3]

Limit of watermarked information is a critical and looked for after subject in the rising patterns of research. Watermarking is has turned into an extremely famous innovation for copyright insurance and validation of electronic archives and media. The purpose behind this may be that there are such a large number of pictures and information accessible in web with no cost, which should be ensured.

Watermarking strategies are favored because of the way that they give trustworthiness to picture and help to keep away from unlawful repetition. Thusly, identification of altering utilizing watermarking strategy has made buzz in the exploration network. In watermarking technique additional data is implanted into the digital piece of picture with the goal that abnormality caused by information lodging stays unrevealed. The supplementary certainty which is installed is designated "watermark". Numerous watermarking calculations see if the first picture has been mutilated or not, some of them can center around the modified zones, while the others have capacity to recuperate changed or altered territories [2].

Any current picture watermark calculation has two attributes: straightforwardness and heartiness. Straightforwardness ensures that the inserted watermark design does not outwardly ruin the first picture dependability and ought to likewise be undetectable. Heartiness ensures that the watermark design isn't sans inconvenience to distinguish and can't be evacuated unlawfully. In addition, any alterations of the picture esteems must be imperceptible, and the watermark technique must be vigorous or delicate with a specific end goal to give security against assailants [4].

At the point when multimedia content is utilized for authoritatively allowed purposes, restorative applications, data detailing, and cash making exchanges, it is fundamental to ensure that the substance started from an unmistakable source and that it was not changed, altered, or misrepresented. This should be possible by settling a watermark in the records. Thus, at the season of checking the picture, the watermark is isolated with the assistance of an unmistakable key connected with the source, and the inventiveness of the data is checked by means of the trustworthiness of the extricated watermark. The watermark can even contain data from the first assume that can help with fixing any adjustment and getting back the first. Plainly, a watermark utilized for confirmation ought not influence the nature of a picture and ought to be impervious to frauds. Heartiness isn't basic in light of the fact that evacuating the watermark renders the substance inauthentic and henceforth valueless.

LITERATURE SURVEY

Security has turned into a constant issue not just in the territories solidly identified with ensured information trade, yet in addition regions associated with information stockpiling. Visual cryptography is the investigation of numerical strategies and fields of data security which enables visual information to be scrambled to such an extent that their unscrambling can be led by the human optical framework, with no muddled cryptographic calculations.

Mandal, J.K. and Ghatak, S., In proposed a novel (2, m + 1) visual cryptographic procedure, where m number of mystery pictures were encoded in view of an arbitrarily created ace as a typical offer for all mysteries which was decodable with any of the offers related to ace offer out of m + 1 produced shares. Rather than creating new pixels for share aside from the ace offer, hamming weight of the squares of the mystery pictures were been adjusted utilizing irregular capacity to produce shares relating to the insider facts. Toward the finish of their work, the proposed plot was secure and simple to execute like other existing procedures of visual cryptography. At the translating end the privileged insights were uncovered by stacking the ace offer on any one offer comparing to the mysteries in any subjective request with legitimate arrangement straightforwardly by human visual framework where shares were imprinted on various transparencies which adjusts the optimality of utilizing shares. The viewpoint proportion and measurement of the mystery pictures and the produced imparts to regard to the source pictures stayed consistent amid the procedure [6]

Quist-Aphetsi Kester developed a cipher calculation for picture encryption of m*n estimate by rearranging the RGB pixel esteems. The calculation makes it practical for encryption and decoding of the pictures in light of the RGB pixel. The calculation was connected effectively without change in the picture estimate and was no loss of picture data after decoding [7].

Koppu and Viswanatham [8] proposed a confused cryptosystem for picture security relying on a Hybrid Chaotic Magic Transform HCMT, which performs picture protection alongside picture encryption and unscrambling. Lanczos calculation is furthermore connected to create a pseudo irregular figure as eigenvalues and eigen vector in low time unpredictability. Pixels are likewise different indiscriminately utilizing half and half CMT strategy with GEM moving.

So the proposed strategy is smarter to confront assaults like differential, savage power, picked plaintext known figure plaintext, key affectability, data entropy, security key space, and furthermore various commotion assaults. The prescribed procedure is much suitable for the protection of 3D helpful pictures and applications which recuperate the rain pictures.

Garg and Kamalinder [9] displayed picture security framework in light of steganography and encryption utilizing AES; a cross breed approach particularly for distributed computing as it is rising on the web stockpiling for clients with slight scruples and tolerance for not overseeing workstation equipment. For steganography, the "cover picture" is actualized in light of shading "enlightenment based estimation" (CIBE), and bits of scrambled pictures are mutilated with minimum critical bits LSBs of every pixel of the cover picture to hide it. One piece variety of unique picture does not impact its value and it appears the genuine picture.

Verma and Jain [10] depicted a less unpredictable calculation to encode pictures utilizing Dual Tree Complex Wavelet Transform which partition the picture into estimation and detail parts. The underlying one is encoded with "pixel confused rearrange method" and next one is anchored utilizing "Arnold Transform". According to the creators' say, the figure is greatly protected regardless of whether its initially is confined without hauling out the calculation, at that point the whole figure can't be accomplished. The replication result additionally clarified that the unscrambled figure at getting end is solely indistinguishable to the first while having entropy contrasts and mean mistakes.

A novel way to deal with digital picture security utilizing cryptosystem with steganography displayed by Azam [11], in which encryption depends on dark scale substitution boxes (sboxes) of RTSs and stage implanting technique. RTSs depend on undisclosed picture pixel estimate fuzzily and of variable size. The spatial and recurrence spaces of the establishment figure are utilized to produce two discretionary covers. The undisclosed picture is established in have picture performing "steganocrypto" concealing systems utilizing two differing RTSs on have picture to create an irregular veil.

At the beneficiary's end, have picture is expected to decode the undisclosed picture, so have picture is likewise scattered with another RTS and embedded with the undisclosed picture. The creator asserts that this "s-box cryptosystem in addition to steganocrypto framework" is a superior cryptosystem contrasted with the current ones and can be utilized for shaded pictures and covering up of information after little alteration.

PROBLEM IDENTIFICATION

1. The issue related with the encryption procedure is that it doesn't give security, once the information is decoded. Watermarking includes, installing the data into the host information, keeping in mind the end goal to give security even after unscrambling.
2. The first fundamental huge disadvantage of data secure plan in view of customary cryptography is illicit sharing of key among sender and recipient, i.e. key dissemination issue.

RESEARCH METHODOLOGY

The proposed method is watermarks is embedded in image and extract the image with secure manner by using security key. The image embedded process is using Pixel wise image embedding technique and the detection phase using block wise detection. Check the image which is marked or not, if the image is watermarked that can be detected and finally the image is recovered. By using watermarking in the image, achieve accurate output image without any attacks.

Pixel-wise embedding method

The focal thought of this technique is to build up a reliance instrument among gatherings of pixels arbitrarily dispersed over the picture, with the goal that any adjustment in a pixel can be altogether identified

by every one of the pixels related to indistinguishable subset from the modified pixel. As a primer advance, the picture lattice X is straightened into a 1 nx exhibit, indicated as X'.

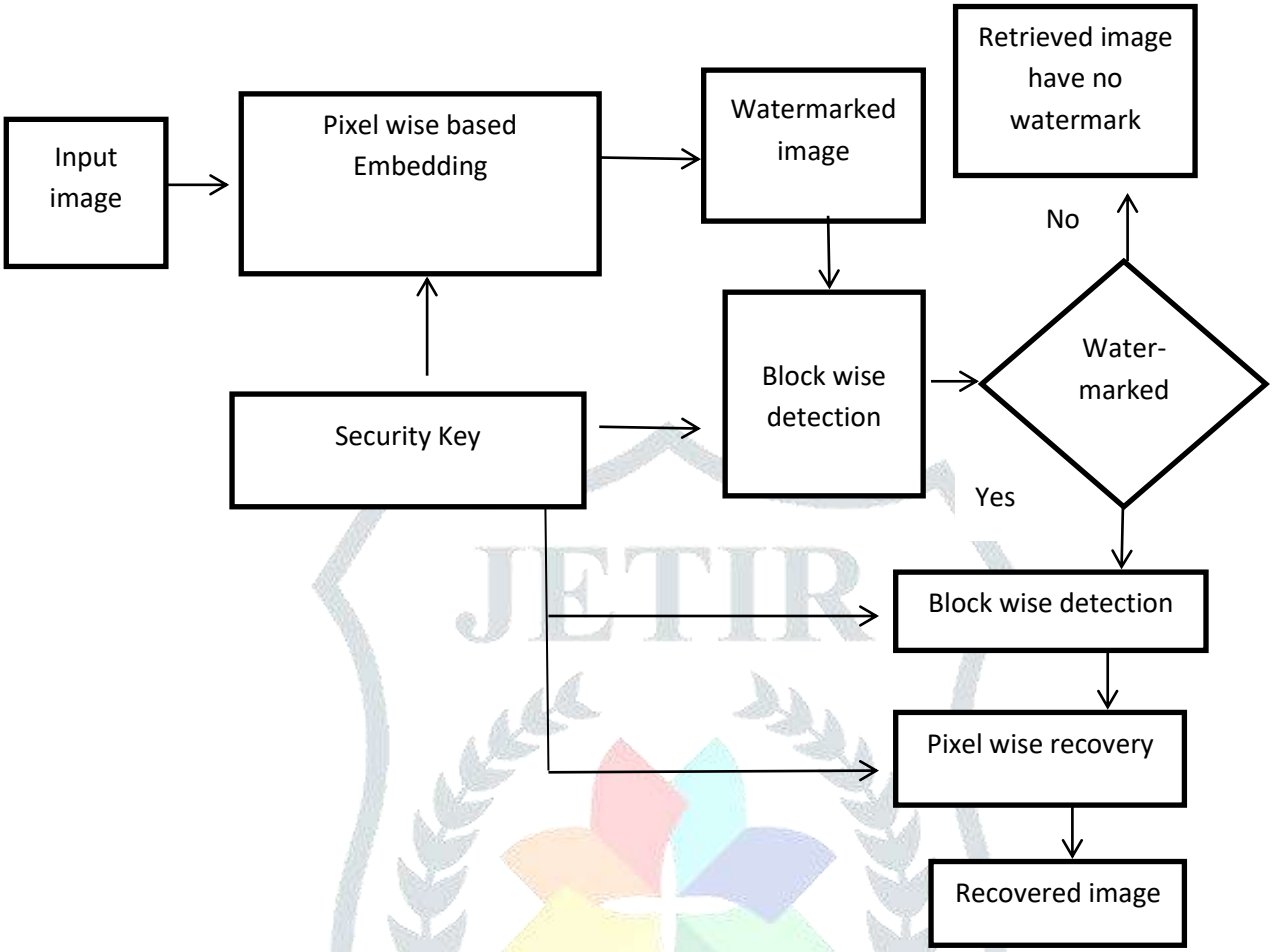

Figure 1 Proposed method

The system depicted underneath will be iteratively rehashed (u-1) times, so an alternate piece plane will be watermarked in every emphasis; let z=u be a whole number that demonstrates the bit-plane to be watermarked in any case. Each emphasis includes the means beneath.

1. A function, S(.), is used to pseudo-randomly shuffle the pixels in X', as $\bar{X} = S(X', \alpha)$, where a is a pseudo-random seed. Next, X is split into non-overlapping arrays of 1 mpw pixels. To compute a different shuffle in each iteration, set $\alpha = (k + z)$, where k is a secret key. This way, every pixel is associated to (u-1) different subsets of pixels.
2. Let $\bar{X}$q be the q-th array, for q=1,….,(n_X/m_{pw}). For each $\bar{X}$q, a bit string W_q, of length m_{pw}, is computed as $W_q = H(k, z, q, \widehat{X_q})$ where H(.) is a cryptographic hash function, $\widehat{X_q} = 2^u \lfloor 2^{-u} \overline{X_q} \rfloor$ and $\lfloor . \rfloor$ denotes the floor function. The parameters k, z, and q are included, in (1), for security reasons. Then, form a $1 \times m_{pw}$ binary array, denoted as Wq, with the bits in wq, and proceed to watermark the z-th bit-plane of $\overline{\text{Xq}}$, by $\widehat{X_q} = 2^z \lfloor 2^{-z} \overline{X_q} \rfloor + 2^{(z+1)} W_q$.
3. Once every single array has been watermarked, return all the pixels to their original location by $X' = S^{-1}(\bar{X}, \alpha)$ where $S^{-1}(.)$is the inverse shuffle function, such that $X' = S^{-1}(S(X', \alpha), \alpha)$.

Next, if z>1 reduce the value of z by one and repeat the procedure to watermark another bit-plane.

4. After (u-1) iterations, update X as an n_1 x n_2 reshaped version of X'.

Block-wise detection method

Consider an n'_1 n'_2 image Y, which is divided into non-overlapping blocks of m_1 x m_2 pixels. For every block Y_r, encode a bit string h'_r, of length m_{bw}, with the LSB of every pixel in Y_r, and compute an authentication bit string,

$$d'_r = H(k, \bar{Y}_r) \oplus h'_r$$

where k' is the secret key, and $\bar{Y}_r = 2\lfloor 2^{-1} Y_r \rfloor$. Let $L(d'_r)$ be a function that retrieves the prefix formed by the γ left-most bits in d'_r. Additionally, let A ={d'_{a1}}, … d'_{af} } be a set of authentication bit strings, such that $L(d'_{a1}) = \cdots = L(d'_{af})$.

If Y is a watermarked, probably tampered, image, and k'= k, it is expected that most of the extracted authentication bit strings will contain the same prefix. Hence, if $a_f \geq \tau_1$, where τ_1 is a predefined threshold, the image is reckoned to be watermarked.

Otherwise, if $a_f < \tau_1$, generate a set of m_1,m_2 different shifted versions of Y. In a shifted version, all the pixels in Y are displaced λ_1 rows and λ_2 columns, where $-m_1 < \lambda_1 \leq 0$ and $-m_2 < \lambda_2 \leq 0$. Every shifted version is analysed as described above in an exhaustive fashion. This way, we can identify cover images whose left and/or upper-most edges have been removed by cropping. If none of the shifted versions was reckoned to be watermarked, the detection process is terminated altogether.

PERFORMANCE ANALYSIS

The performance analyses of the proposed method are calculating the image which is watermarked or not, parameter used to calculate the images are Mean square error (MSE), Peak Signal Noise Ratio (PSNR).

Mean square error (MSE)

The mean squared error (MSE) in an image watermarking is to estimate or measures the average of the squares of the "errors", between host image and watermark image.

$$MSE = 1 \div MN \sum_{i}^{M} \sum_{j}^{N} (W_{ij} - H_{ij})^2$$

Where M, N is pixel values in host image

W_{ij}= Pixel value in Watermarked Image

H_{ij}= Pixel value in Host Image

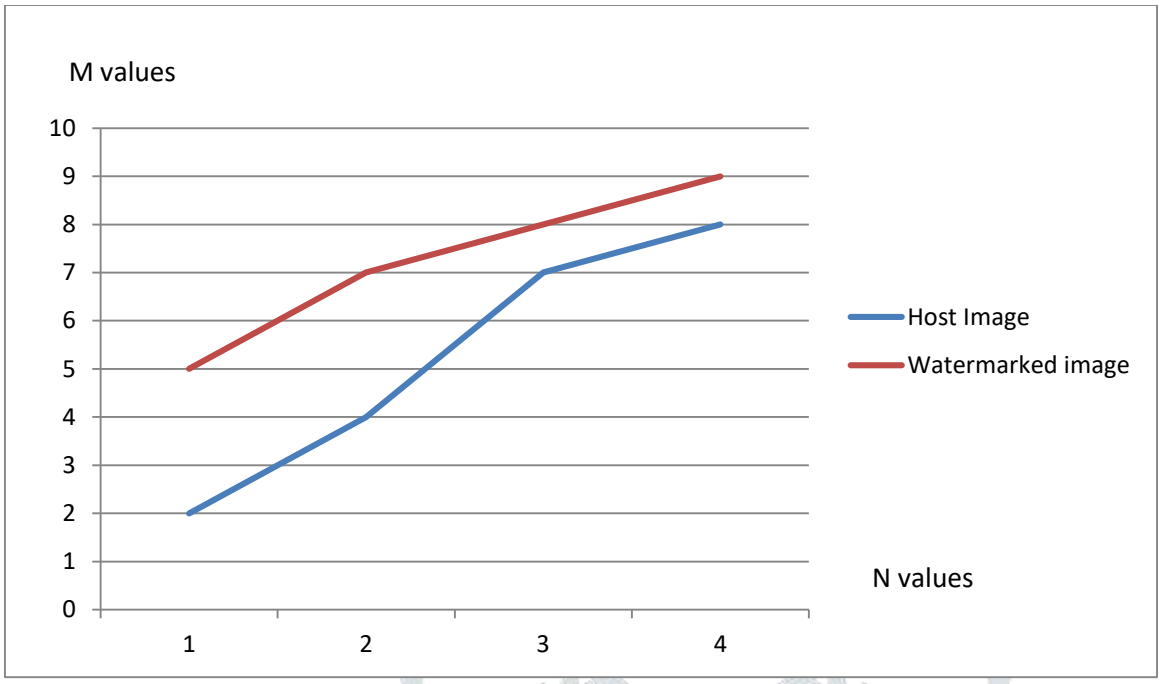

Figure 2 Performance of *Mean square error (MSE)*

Peak signal to noise ratio (PSNR)

PSNR (Peak Signal to Noise Ratio) is used to determine the Efficiency of Watermarking with respect to the noise. The noise will degrade the quality of image. The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio. It is given by

$$PSNR = 10 * log\ (P^2/MSE)$$

Where p= maximum value in host image.

Imperceptibility of image is determined by this factor. More the PSNR shows that Watermarked image is perceptible or watermark is not recognized by naked eyes.

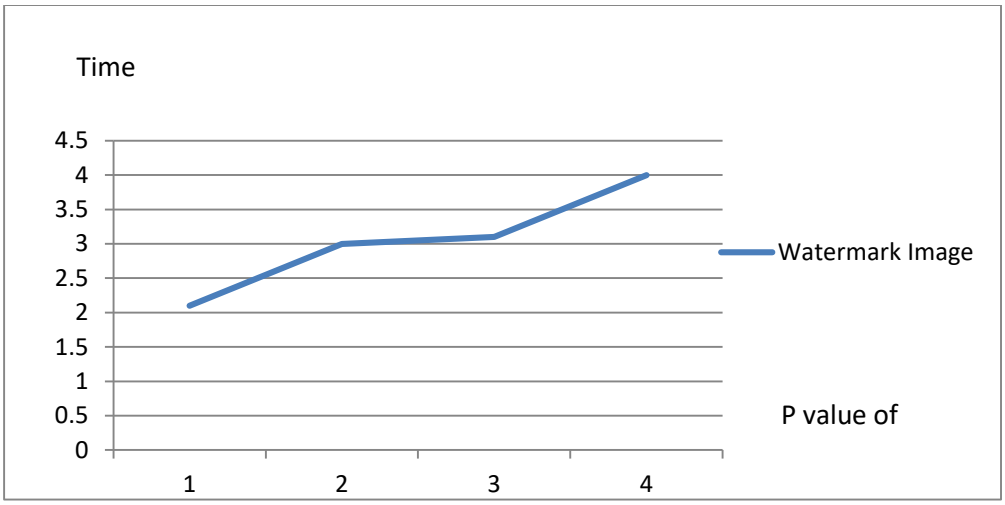

Figure 3 Peak signal noise ratio graph

CONCLUSION

The uses of "digital watermarking" have grown to becoming extensive in the contemporary Information and Communications Society (ICS). Digital watermarking techniques used for security o and copyright protection of still image. There are many techniques use in practice to provide the copyright protection such as digital watermarking technique. In this paper, we discuss the protection of image from hackers by using watermarking technique called pixel based embedding and block wise detection technique used. The performance analysis of the proposed method is calculating the image which is watermarked or not based on the PSNR and SME value.

REFERENCE

1. Lalit Kumar Saini1, Vishal Shrivastava, " A Survey of Digital Watermarking Techniques and its Applications' International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

2. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN), ISBN: 0-7803-9094-6, pp. 709-716,IEEE 2005.

3. Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

4. Adel Hammad Abusitta, "A Visual Cryptography Based Digital Image Copyright Protection", Journal of Information Security, 2012, 3, 96-104.

5. Blesswin, J.; Rema; Joselin, J., "Recovering secret image in Visual Cryptography," Communications and Signal Processing (ICCSP), 2011 International Conference on , vol., no., pp.538,542, 10-12 Feb. 2011

6. Mandal, J.K.; Ghatak, S., "A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography (SCOSVC)," Electronic System Design (ISED), 2011 International Symposium on , vol., no., pp.329,334, 19-21 Dec. 2011

7. Quist-Aphetsi Kester,"Image Encryption based on the RGB PIXEL Transposition and Shuffling",IJCNIS, vol.5, no.7, pp.43-50,2013. DOI: 10.5815/ijcnis.2013.07.05

8. S. Koppu, and V. M. Viswanatham, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform", Modelling and Simulation in Engineering, vol. 2017, pp. 1-12, 2017

9. A. Verma, and A. Jain, "Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform", Journal of Network Communications and Emerging Technologies, Vol. 6, Issue 5, pp. 8-11, 2016.

10. N. Garg, and K. Kaur, "Hybrid information security model for cloud storage systems using hybrid data security scheme", International Research Journal of Engineering and Technology, Vol. 3, Issue 4, pp. 2194-2196, 2016

11. N. A. Azam, "A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding", Security and Communication Networks, Vol. 2017, pp. 1-9, 2017.

12. Sudhanshu Suhas Gange, Ashok A.Ghatol, "Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014.

13. Sergio Bravo-Solorio, Asoke K. Nandi, "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities" Elsevier Signal Processing 2010.

14. Adel Hammad Abusitta, " A Visual Cryptography Based Digital Image Copyright Protection" , *Journal of Information Security*, Vol. 3, Page Number 96-104, 2012.

15. S Chakrabarti, D Samanta, "Image Steganography Using Priority-Based Neural Network and Pyramid", Springer(Singapore), Emerging Research in Computing, Information, Communication and Applications(2016), pp 163-172

16. Jian Ren, "A cryptographic watermarking technique for multimedia signals", Springer, Adv Comput Math (2009) 31:267–281