United International Journal of Engineering and Sciences
(UIJES – A Peer-Reviewed Journal); ISSN:2582-5887 | Impact Factor:8.075(SJIF)
Volume 5 | Special Issue 1 | 2025 Edition
National Level Conference on "Advanced Trends in Engineering Science & Technology" – Organized by RKCE

A-Fast-Image-Dehazing-Algorithm-Using-Morphological Reconstruction

Dr. MANJUNATH B E[1]

Professor[1], [234]UG scholar

SHARADHA D[2], L NIKITHA[3], B SRAVANI[4], C NONVITHA[5]

Department of Electronics Communication Engineering
R K College of Engineering
Vijayawada, India

Abstract:
Traditional permutation encryption algorithm is not robustness for noise disturbing and shear transformation attacks. In order to ameliorate the security of image encryption algorithm, we present an image encryption algorithm based on location transformation. The algorithm permute image based on chaotic system and storage everyone pixel of the image in multi-place, this encrypted image is robustness for noise disturbing and shear transformation attack. An extended magic square matrix-generating algorithm is also presented and it improves on the efficiency of the magic square matrix-generating algorithm. The simulation results show that the effect of decrypting image is good when the encrypting image is modified by noise disturbing and shear transformation attack

I.INTRODUCTION

Watermarking (data hiding) is the process of embedding data into a multimedia element such as image, audio or video. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or a detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark and its affect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks, and normal A/V processes such as noise, filtering (blurring, sharpening, etc.), resampling, scaling, rotation, cropping, and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark. The approaches used in watermarking still images include least-significant bit encoding, basic M-sequence, transform techniques, and image-adaptive techniques.

An important criterion for classifying watermarking schemes is the type of information needed by the detector:

- Non-blind schemes: Both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes: The secret key(s) and the watermark bit sequence.
- Blind schemes: Only the secret key(s).

Typical uses of watermarks include copyright protection (identification of the origin of content, tracing illegally distributed copies) and disabling unauthorized access to content. Requirements and characteristics for the digital watermarks in these scenarios are different, in general. Identification of the origin of content requires the embedding of a single watermark into the content at the source of distribution. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in the multimedia network. In both of these applications, non-blind schemes are appropriate as watermark extraction or detection needs to take place in a special laboratory

environment only when there is a dispute regarding the ownership of content. For access control, the watermark should be checked in every authorized consumer device used to receive the content, thus requiring semi-blind or blind schemes.

Note that the cost of a watermarking system will depend on the intended use, and may vary considerably. Two widely used image compression standards are JPEG and JPEG2000. The former is based on the Discrete Cosine Transform (DCT), and the latter the Discrete Wavelet Transform (DWT). In recent years, many watermarking schemes have been developed using these popular transforms.

In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be least resistant to attacks. In image watermarking, two distinct approaches have been used to represent the watermark. In the first approach, the watermark is generally represented as a sequence of randomly generated real numbers having a normal distribution with zero mean and unity variance. This type of watermark allows the detector to statistically check the presence or absence of the embedded watermark. In the second approach, a picture representing a company logo or other copyright information is embedded in the cover image. The detector actually reconstructs the watermark, and computes its visual quality using an appropriate measure.

A few years ago, a third transform called Singular Value Decomposition (SVD) was explored for watermarking. The SVD for square matrices was discovered independently by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. It was not used as a computational tool until the 1960s because of the need for sophisticated numerical techniques. In later years, Gene Golub demonstrated its usefulness and feasibility as a tool in a variety of applications. SVD is one of the most useful tools of linear algebra with several applications in image compression, watermarking, and other signal processing fields.

A DWT-based multiple watermarking argues that embedding a visual watermark in both low and high frequencies results in a robust scheme that can resist to different kinds of attacks. Embedding in low frequencies increases the robustness with respect to attacks that have low pass characteristics like filtering, lossy compression, and geometric distortions while making the scheme more sensitive to modifications of the image histogram, such as contrast/brightness adjustment, gamma correction, and histogram equalization.

Watermarks embedded in middle and high frequencies are typically less robust to low-pass filtering, lossy compression, and small geometric deformations of the image but are highly robust with respect to noise adding, and nonlinear deformations of the gray scale. Arguing that advantages and disadvantages of low and middle-to-high frequency watermarks are complementary, the authors propose a new scheme where two different visual watermarks are embedded in one image. Both watermarks are binary images, one contains the letters CO, and the other EP against a white background. The cover image is the picture of a young girl. Two levels of decomposition are performed on the cover image. The watermark CO is embedded in the second level LL, and the watermark EP is embedded in the second level HH. The experiments show that embedding in the LL sub band is robust against JPEG compression, wiener filtering, Gaussian noise, scaling, and cropping while embedding in the HH sub band is robust against histogram equalization, intensity adjustment, and gamma correction. Extracted watermarks appear to have similar quality after the Gaussian noise

attack only. We noticed that the embedded watermark is highly visible in all parts of the cover image. The degradation is pronounced especially in low frequency areas (e.g., the wall behind the young girl), resulting in a loss in the commercial value of the image.

In the project, we generalize the above scheme to four sub bands using DWT-SVD watermarking.

II. LITERATURE SURVEY

2.1 DATA ENCRYPTING IN A BINARY IMAGE BASE ON MODIFIED DATA HIDING METHOD

This encryption technique controls sub-partitioned squares utilizing altered piece position to supplant a mystery bit. The sub-separated square contains at least three pixels of the host paired picture. For each square chooses to shroud a mystery bit. By finding the pixel position to embed a mystery bit for each square, the picture nature of the obvious parallel picture can be improved.

2.2 ENCRYPTING PROCESSES

Give H a chance to be the host double picture of MXN pixels and C be the mXn-bit mystery information. For pixel esteem h(i,j) of H, another pixel worth is characterized as h'(i,j). The accompanying procedures are executed to shroud an information bit.

1. For a given H. Select a sub-partitioned square Buv with size pXq for concealing a mystery information bit.
2. Summing all pixels of Buv.
3. If S(Buv) is equivalent to 0 or pXq, isn't utilized to store a mystery information bit in the square.
4. If mod(S(Buv),2) is equivalent to the C(z), at that point don't roll out an improvement and spare the information bit in this square.
5. If mod(S(Buv),2) isn't equivalent to the C(z),

2.3 ENCRYPTING PROCESSES

Give H a chance to be a host twofold picture and let H* be a plain double picture changed from H. The components of the clear picture H* contain encoded codes and the codes are arranged into five gatherings of codes. The recognizable proof codes are utilized to decide whether the codes scrambled in H* utilize the encoded strategy proposed in this paper or not; the underlying position codes are utilized to dole out the underlying position of the upper left of the sub-separated square; the sub-isolated square measurement codes are utilized to show the size of the sub-partitioned obstruct; the secretive double picture measurement codes are utilized to demonstrate the size of the incognito parallel picture; (all the previously mentioned codes situate at the main column to the second one of H*) the data codes are utilized to decode undercover twofold picture (situate at the third line to the last one of H*). ID codes resemble passwords and they are utilized to decide if a plain picture contains codes proposed in this paper or not. Distinguishing proof codes are made out of 20-bit of pseudo-arbitrary paired codes, for example 10011000010000100001. Introductory position codes are utilized to allocate the underlying position of the upper left of the sub-isolated square and they need two arrangements of 4-bit twofold codes. The primary set demonstrates the quantity of the line position and the subsequent set demonstrates the quantity of the section position. The codes 0000, 0011, 0111, and 1111 are utilized to speak to number of 1, 4, 8, and 16, individually. Other number codes can be utilized correspondingly.

2.4 VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES

Cryptography includes changing over a message content into an incoherent figure. Then again, steganography implants message into a spread media and conceals its reality. Both these methods give some security of information neither of only them is secure enough for sharing data over an unbound correspondence channel and are helpless against gatecrasher assaults. In this paper we propose a propelled arrangement of scrambling information that joins the highlights of cryptography, steganography alongside mixed media information stowing away. This framework will be more secure than some other these procedures alone and furthermore when contrasted with steganography and cryptography joined frameworks.

1. Encryption Algorithm: The message will initially be scrambled utilizing Asymmetric Key Cryptography system. The information will be encoded utilizing essential DES calculation. This figure will presently be covered up into a sight and sound record. The figure will be spared in the picture utilizing an altered piece encoding strategy by truncating the pixel esteems to the closest zero digit (or a predefined digit) and afterward a particular number which characterizes the 3-D portrayal of the character in the figure code arrangement can be added to this number. For each character in the message a particular change will be made in the RGB estimations of a pixel. (This change ought to be under 5 for each of R,G and B esteems) This deviation from the first worth will be novel for each character of the message. This deviation likewise relies upon the particular information square (lattice) chose from the reference database. For every byte in the information one pixel will be altered. In this way one byte of information will be put away per pixel in the picture. In this strategy the figure arrangement can be decoded without the first picture and just the altered picture will be transmitted to the collector. In the initial couple of lines of picture properties, the qualities of the picture will be encoded and spared in order to give us the data if the picture is altered or adjusted or the picture augmentation has been changed like jpg to gif. These properties can be utilized in the translating (distinguishing the right square of information from the information lattice). So just the right encoded picture in the right arrangement will deliver the sent message. For unscrambling, the beneficiary must realize which picture to decipher and in which arrangement as changing the picture configuration changes the shading dispersion of the picture. Each picture gives an irregular information on decoding that has no significance. Yet, just the right organization unscrambling gives the first message. In the wake of concealing the information in the picture, the picture will be sent to the collector. The recipient ought to have the unscrambling key (private key) which will be utilized to interpret the information.

2. Unscrambling Algorithm: The message can be decoded utilizing a backwards work (as utilized in customary strategies) utilizing the recipient's private key. This key can be a piece of the picture or a content or any trait of the picture. The beneficiary's private key is utilized to distinguish the reference framework from the reference database. Subsequent to choosing the right matrix, the x and y part of the picture can characterize the square that has been utilized to encode the message and the RGB esteems can point to the information in the square distinguished by the x, y segment. The figure is recovered by getting the distinction in the pixel esteem from the nearest predefined esteem (zero truncation). These numbers will currently characterize the spared bit and will shape the figure content. This figure would now be able to be unscrambled utilizing a backwards capacity of the DEA calculation to get the message content..

2.5 IMAGE STEGANOGRAPHY USING MOD-4 EMBEDDING ALGORITHM BASED ON IMAGE CONTRAST

So as to improve the limit of the shrouded mystery information and to give a vague stego picture quality, another picture steganography technique dependent on picture difference is displayed. A gathering of 2×2 squares of non-covering spatially neighboring pixels is chosen as the substantial square for installing the mystery message. The modulo 4 number juggling task is additionally connected to all the substantial squares to install a couple of twofold bits utilizing the briefest course change conspire. Every mystery message is likewise encoded by RSA encryption calculation to furnish the framework with greater security.

Encryption: In this segment we propose a RSA open key encryption for encoding the mystery message before implanted into spread picture. RSA can be utilized for both encryption and unscrambling. In open key encryption the sender will utilize the open key during the encoding procedure and just the private key, which has a direct numerical association with the open key, can decode the mystery message. Open key encryption is the most secure kind of steganography. It additionally has numerous degrees of security in that undesirable gatherings should initially associate the utilization with steganography and after that they would need to figure out how to break the calculation utilized by the open key framework before they could catch the mystery message.

Information Hiding: In this segment we propose a mod-4 implanting technique for data stowing away inside the spatial area of any dim scale picture. This technique can be considered as the improved adaptation of. The information messages can be in any computerized structure, and are frequently treated as a bit stream. Installing pixels are chosen dependent on some scientific capacity which relies upon the pixel force estimation of the legitimate squares in a picture. Before implanting a looking at has been done to discover whether the chose installing pixels lies at the limit of the picture or not. Information implanting are finished by mapping every two bits of the mystery message in every one of the legitimate square dependent on certain highlights of that pixel.

Information Hiding Model: The info messages can be in any computerized structure, and are regularly treated as a bit stream. The information message is first changed over into scrambled structure through proposed encryption technique. This encoded message produces the mystery key which might be utilized as a secret word before beginning of the implanting or extricating activity for expanding another degree of security. Second the picture is reshaped to the 2×2 squares of non-covering spatially adjoining pixels. At that point the substantial squares are chosen from these squares. Square Q is legitimate if the normal contrast between the dark level values of the pixels of that and it's mean (C) exceeds a threshold (minimum contrast)

2.6 IMPLEMENTATION AND ANALYSIS OF THREE STEGANOGRAPHIC APPROACHES

This paper proposes the improve security framework by joining these two systems. In this framework, the scrambled message is installed in a BMP picture document. In proposed framework, three LSB steganographic strategies have been executed and broke down. This proposed framework means for information secrecy, information validation and information trustworthiness. This framework upgrades the security of information as well as turns out to be all the more dominant instrument. This framework expects to help successful ways for ensuring information. The essential objective of our framework is to improve the security of information and afterward to think about three steganographic methods. At that point we will utilize the advanced technique for implanting. In this paper, we simply present three steganographic approaches. In this framework, information is encoded with RC4 encryption calculation and after that inserted the scrambled content in the BMP picture record utilizing three steganogrpaphic techniques.

III. EXISTING SYSTEM

CRYPTOGRAPHY

Cryptography is a craft of securing the data by changing into an indiscernible and untraceable configuration known as figure content. Just the individual who have the mystery key can interpret or we can say unscramble the message into the first structure. Cryptography is the strategy by which one can send and share the data in a mystery way. Due the cryptography the data is by all accounts seeming like a trash worth and it is in every case practically difficult to discover the data substance lying under the picture or a video document. The data looks like covered up inside the picture or the video document. A most straightforward and surely understood calculation for cryptography is as appeared in fig 2. The encryption key generator is utilized to produce the encryption key just as the open key as appeared in the beneath square chart. By utilizing the encryption key the data substance to be sent gets encoded by the encryptor. The encoded data is then transmitted to the specific recipient. At the recipient end the cryptography decryptor is utilized which concentrates the first data substance mapped onto the picture or a video document with the assistance of an open key given by the transmitter segment. By the utilization of the cryptography technique just, the collector which has the learning of the open key can recover the first data content from the picture or a video record. So regardless of whether any undesirable individual or a source gets the picture or a video document with data substance covered up in it, it can't be extricated without appropriate open key. So open key assumes a fundamental job in the entire cryptography process.

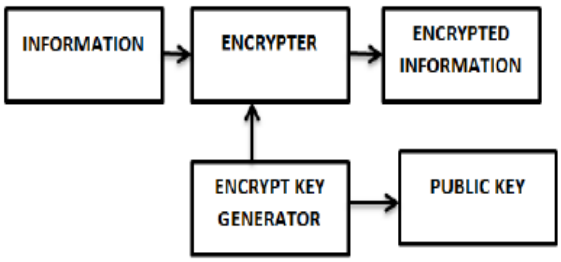


Fig.4.1. encrypter

In fact in one bit of information inside another". Present day the chance of concealing data into advanced mixed media documents and furthermore at the system bundle level. Concealing data into a media requires following components. The spread media(C) that will hold the shrouded information

1. The mystery message (M), might be plain content, figure content or any kind of information
2. The stego work (Fe) and its converse (Fe-1)
3. An discretionary stego-key (K) or secret key might be utilized to stow away and unhide the message .

Cryptography is the workmanship or investigation of concealing data by embeddings mystery messages in different messages. Medium where data is embedded can be anything. This medium is known as the spread article. Cryptography that is connected to shroud data on the front of advanced articles is called Digital Cryptography. Spread items that are utilized in computerized cryptography can differ, for instance in the picture document. Cryptography calculations in the picture chronicle

have been broadly created. In the mean time, cryptography calculations in sound chronicle are generally few. As of late there are such a significant number of calculation have been created to give greater security, improved quality with simple usage and quicker figurings. Among them the majority of the strategies have their very own downsides like computational unpredictability, time utilization and remaking of mystery data and so on., Here, in this proposition we executed pixel mapping based video steganography, which is an extremely straightforward and simple estimations and furthermore give greater security.

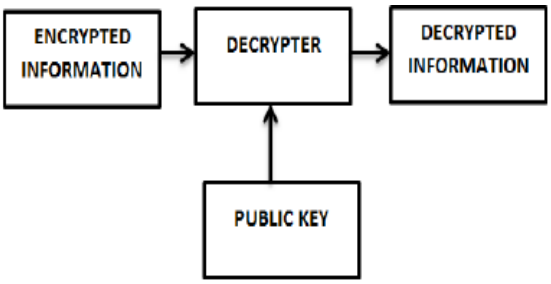


Fig. decrypter

III. PROPOSED SYSTEM

Proposed techniques for the simulation results show that when noise disturbing attacks the encrypted image or shear transformation attacks the encrypted image, the corresponding decrypted image's information is destroyed. This means that the above permutation transform is not robustness for noise disturbing and shear transformation attack. In order to solve this problem and ameliorate the robustness of the above image encryption algorithm we will propose a new method, the main idea is to storage everyone pixel of the image in multi-place. The ameliorated algorithm is described as follow.The remaining of the paper will be organized as follows. Firstly, we will provide a brief introduction to integer wavelet transform. Secondly we will describe the proposed encryption system. Then, we will discuss the achieved results; and finally we will conclude the paper and suggestfuture improvements to the system

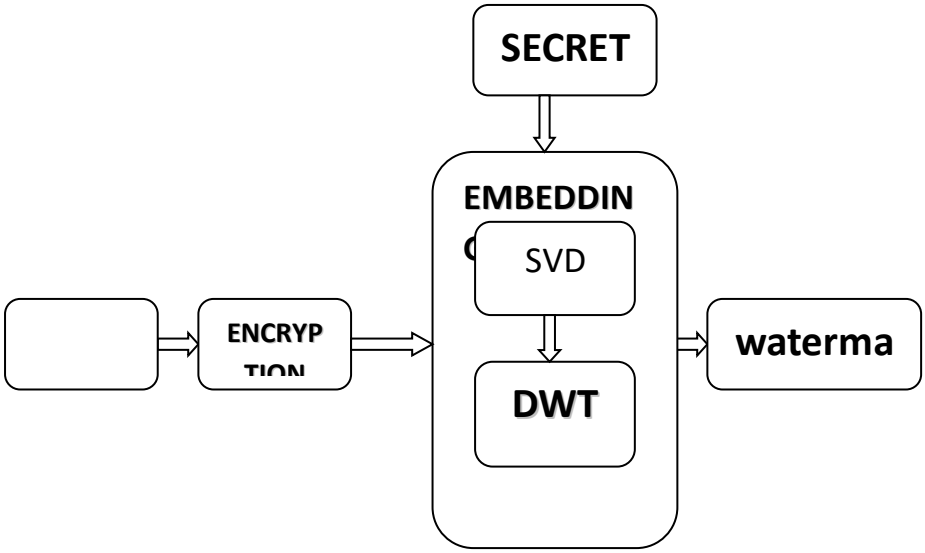
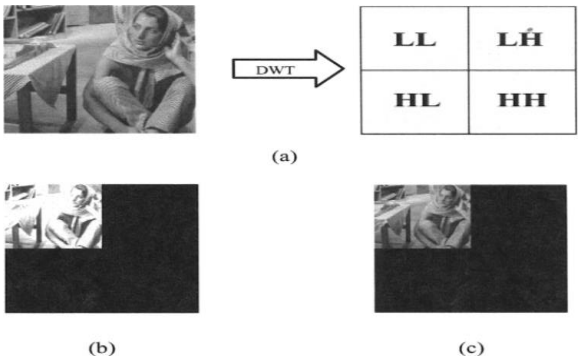


Fig: proposed system

DISCRETE WAVELET TRANSFORM

wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system . To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image and in this case there will be no loss of information through forward and inverse transform [II]. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL sub band in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted as shown in "Fig. I".



Lifting schemes is one of many techniques that can be used to perform integer wavelet transform it is also the
scheme used in this paper. The following is an example showing how we can use lifting schemes to obtain integer
wavelet transform by using simple truncation and without losing invertibility
The HAAR wavelet transform can be written as simple pair-wise averages and differences

From experiments we found that as we lower the bits used to hide the secret message in the LL subband the resulted distortion in the stego-image becomes lower; so that we modified this hiding capacity function by using different

ranges for k for the LH, HL and HH subbands where its values are form 1 to 4. For the LL subband the value of k is equal to 0 and in some cases the bits used is fixed to only bits to enhance the stego-image quality. Form experiments of different values of k we divided the system into 3 cases of operation depending on the requirements of the user; these cases are
Case 1: k 1 for LHI, HLI and HH 1 sub bands, while using 2 bits for embedding data in LL 1 sub band This case provides low hiding capacity with high visual quality of the stego-image.
Case 2: k 3 for LHl, HLI and HHI subbands, while using 2 bits for embedding data in LL 1 subband This case is for applications requiring average hiding capacity with reasonable visual quality
Case 3: k 4 for LHl , HLI and HHI sub bands, while k = 0 for LLI subband) Case 3 is considered as the worst case of data embedding where it is used when the high visual quality of the stego image is not important and the user requires only high hiding capacity.

Note that we dropped the case of k=2 because it provided no significant improvements to the results obtained by k=l or k=3. To realize how we use the hiding capacity function; for example, If L=3, then the three least significant bits of the wavelet coefficient will be replaced with three bits of the message data.

Step 6: Embed L bits of message into the corresponding randomly chosen coefficients. Random selection of coefficients provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.

Step 7: Apply optimal pixel adjustment algorithm, while taking into consideration that each modified coefficient stays in its hiding capacity range where each value of L is calculated according to the absolute value of the wavelet coefficients any significant change in this value will produce different value of L to be calculated at the receiver. The main idea of using the optimum pixel adjustment (OP A) algorithm is to minimize the error difference between the original coefficient value and the altered value by checking the right next bit to the modified LSBs so that the resulted change will be minimal For example, if a binary number 1000 (decimal number 8) is changed to 1111 (decimal number 15) because its three LSB's were replaced with embedded data; the difference from the original number is 7. This difference in the original value is called the embedding error. By adjusting the fourth bit from a value of I to a value of 0, the binary number now becomes 0111 (decimal number 7) and the embedding error is reduced to I while at the same time preserving the value of the three embedded bits.

The algorithm we used in [4] is the final step in the proposed scheme, where it can minimize the error by half. The main idea of OP A is to check the bit right next to the last changed LSBs is used to decrease the error resulted after insertion of message bits. The algorithm according to depend on calculating the difference (OJ) between original value P(x, y) and the modified value P'(x, y)

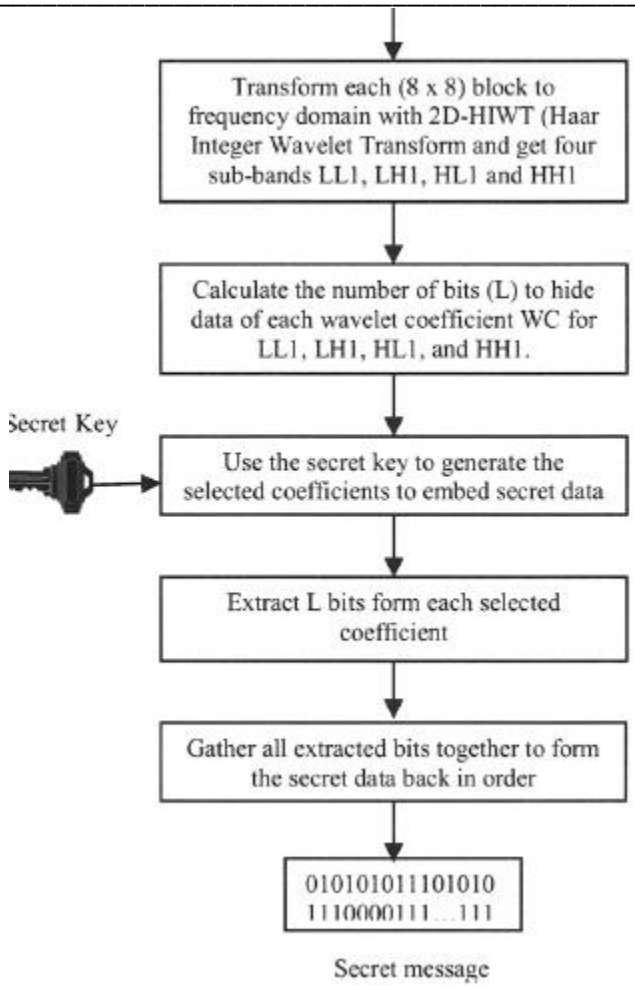


Figure 3. The block diagram of the extraction algorithm

IV. CONCLUSION

This work proposes a lossless, a reversible, and a consolidated information concealing plans for figure content pictures encoded by open key cryptography with probabilistic and homomorphic properties. In the lossless plan, the figure content pixel esteems are supplanted with new qualities for implanting the extra information into the LSB-planes of cipher text pixels. Along these lines, the implanted information can be legitimately extricated from the scrambled area, and the information inserting task does not influence the unscrambling of unique plaintext picture. In the reversible plan, a pre processing of histogram therapist is made before encryption, and a half of cipher text pixel esteems are altered for information installing. On collector side, the extra information can be removed from the plaintext space, and, in spite of the fact that a slight contortion is presented in unscrambled picture, the first plaintext picture can be recuperated with no mistake. Because of the similarity of the two plans, the information implanting activities of the lossless and the reversible plans can be at the same time performed in an encoded picture. In this way, the collector may remove a piece of installed information in the scrambled space, and concentrate another piece of implanted information and recuperate the first plaintext picture in the plaintext area.

V. REFERENCES

[1]N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.

[2] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing,

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.

[6] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316−325, 2013.

[7] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.

[8] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.

[9] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.

[10] X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013.

[11] X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters, 18(4), pp. 255−258, 2011.

[12] W. Hong, T.-S.Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, 19(4), pp. 199−202, 2012.

[13] J. Yu, G. Zhu, X. Li, and J. Yang, "An Improved Algorithm for Reversible Data Hiding in Encrypted Image," Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012), Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013.

[14] W. Puech, M. Chaumont, and O. Strauss, "A Reversible Data Hiding Method for Encrypted Images," Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.