International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Highly Secured Lossless Image Cryptography Algorithm Based on Haar Wavelet Transform

Rishi Kumar Gupta[1], G. Sujatha[2]

[1]M.Tech, SRM University Chennai, India

[2]Assistant Professor, SRM University Chennai, India

Abstract: ***Along with the rapid increasing growth of computer and network technologies, images are being transmitted more and more frequently. Security of image is a big issue. Image information is lively and visual, and has been an important means of expressing information of person. There are many encryption algorithm had been available each one having some strength and weakness. Image cryptography can use text cryptosystems to encrypt images directly, since image size is greater than text. Image encryption can be classified into lossy and lossless encryption methods. Lossless encryption methods are more applicable than lossy encryption methods when marginal distortion is not tolerable. In the proposed system, find the hash value of image using by image hashing toolbox. Image hashing is very easy to the tamper with digital data without leaving any clues. Under these circumstances, integrity verification has become an important issue in the digital world. After finding the hash value, the image is transformed into the frequency domain using the wavelet transform, Image processing and analysis based on the continuous or discrete image transforms are classic techniques. The image transforms are widely used in image filtering, data description, etc. Nowadays the wavelet theorems make up very popular methods of image processing, de-noising and compression. The image transform theory is a well-known area characterized by a precise mathematical background. Considering that the Haar functions are the simplest wavelets, these forms are used in many methods of discrete image transforms and processing then the image sub-bands are encrypted in a such way that guarantees a secure, reliable, and an unbreakable form. The encryption involves scattering the distinguishable frequency data in the image using a reversible weighting factor amongst the rest of the frequencies. The algorithm is designed to shuffle and reverse the sign of each frequency in the transformed image before the image frequencies are transformed back to the pixel domain. The decryption algorithm reverses the encryption process and restores the image to its original form.***

Keyword: Wavelets, Haar Transform, Lossless image encryption/decryption, Symmetric key encryption, Image hashing, Block based matrix transformation.

1. Introduction

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is an effective way of protecting sensitive data stored on media or transmitted over unsecured network communication paths. With the rapid development of communication and internet technology, there is always a growing concern about the security of multi-media information such as image. A major challenge is to protect the confidentiality and integrity of such images so that the visual data cannot be misused. Applications like information storage, information management, patient information security, satellite image security, telemedicine, military information security etc. which require information security. Different cryptographic methods are used by different organization for protecting their confidential data. But cryptography hackers are always trying to break the cryptographic method. For this reason cryptographers are trying to develop new cryptographic method to keep the data safe as far as possible. For this reason, cryptographers are always trying to propose new methods and techniques to keep data/information secure. Until now, several data encryption algorithms had been presented such as DES, AES, IDEA, RSA, etc. most of which are used for encrypting text data. It is not suitable to use them for multimedia data because multimedia data is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Image encryption methods can be classified into either lossy or lossless. In lossy encryption methods, were the image details are somewhat distorted, the resulting decrypted image is different from the original image. Due to the characteristics of human perception, and depending on the application, a decrypted image with little distortion is usually acceptable. However, lossless encryption methods are more applicable in applications where the distorted-free original image is required. If attacker tempers or modifies the image's sub band than target user cannot analyzed that receiving image is original or not. So by hashing we can provide the integrity as well as authenticity to the image over the unsecure network. In the proposed algorithm, the image is transformed into the frequency domain using the Discrete Wavelet Haar Transform (DWT) with two levels of decomposition, where the image sub-bands are processed in such a way that ensures that the original image can never be recovered without using the proposed decryption algorithm. The image decryption is also applicable in the frequency domain where the image sub-bands are converted back to their original form by reversing the encryption process.

2. Spatial Frequency Transformation

We have deal with images in many domains. Now we are processing signals (images) in frequency domain. Since this Haar wavelet and frequency domain is purely mathematics. In spatial domain, we deal with images as it is. The value of the pixels of the image change with respect to scene. Whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain.

Spatial Domain: In simple spatial domain, we directly deal with the image matrix.

Frequency Domain: We first transform the image to its frequency distribution. Then our black box system performs whatever processing it has to performed, and the output of the black box in this case is not an image, but a transformation. After performing inverse transformation, it is converted into an image which is then viewed in spatial domain

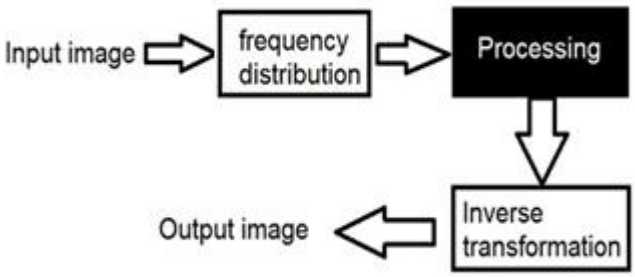

Figure: Image processing in Frequency Domain

In this research, the DWT Haar transform is used. Proposed algorithm is simple, effective, and secure. Compared to the rest of the algorithms in this domain, the proposed algorithm introduces lossless image cryptography that surpasses the lossy algorithms by preserving every single detail in the image; hence it is the category under which this research falls. The purpose of image transformation is to represent the image's highly correlated data in another decorrelated form, by switching from the spatial to the frequency domain. Any transformation technique should be reversible and computationally tractable with low memory requirement and a low number of arithmetic operations. Image based transform methods yield better results at the cost of extra complexity, so in this research, DWT is chosen as the transformation method.

3. Image Hashing

Hash functions are frequently called message digest functions. Their purpose is to extract a fixed-length bit string from a message (image, documents, etc.). Hash functions have found varied applications in various cryptographic, compiler and database search applications. In cryptography, hash functions are typically used for digital signatures to authenticate the message being sent so that the recipient can verify its source. Recently, there has been a lot of interest in using hash functions in multimedia applications both for security and indexing. A key feature of conventional cryptographic hashing algorithms such as message digest 5 (MD5) and secure hash algorithm 1 (SHA-1) is that they are extremely sensitive to the message, i.e. changing even one bit of the input will change the output dramatically. However, multimedia data such as digital images go through various manipulations such as compression, enhancement, cropping, and scaling. An image hash function should instead take into account the changes in the visual domain and produce hash values based on the image's visual appearance. Such a hash function would be useful in identifying images in databases, in which the image possibly undergoes incidental changes (such as compression and format changes, common signal processing operations, scanning or watermarking). A second significant application of a perceptual image hash could be for robust image authentication. In such cases, the hash must be invariant under perceptually insignificant modifications to the image but detect malicious tampering of image data. Several other applications can be identified in the areas of watermarking and information embedding in images.

4. Encryption Algorithm

The encryption algorithm uses the DWT to encrypt the image and compute (wavelet decomposition) the approximation coefficients matrix and details coefficients matrices of the target (original) image using the Haar transform in the first wavelet decomposition. The approximation coefficients matrix is then used to produce the second wavelet decomposition, i.e. encryption process repeated again on the 1st level of wavelet decomposition. The use of two-levels of wavelet decompositions keeps the algorithms' complexity low, i.e., lower number of computations compared to N-levels of wavelet decompositions. Weighting factor can be used as the encryption key in this algorithm. In proposed system 2-levels inverse discrete wavelet transform (IDWT) of the image is performed. The image frequencies are transformed back to the pixel domain, with the pixel values changed and the image details concealed.

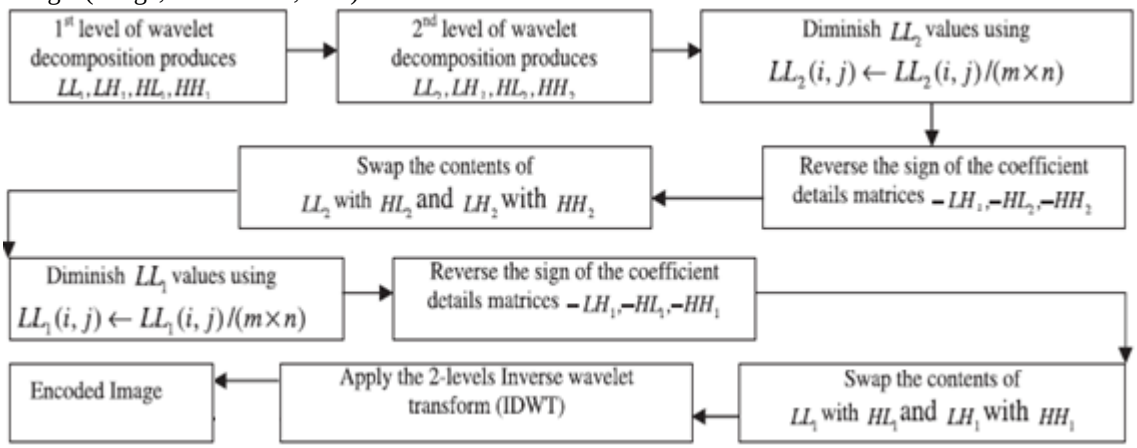

Figure: A flowchart of the proposed image encryption algorithms

There are following steps of encryption algorithm:

- Weighting factor can be used as the encryption key in this algorithm.
- 1st level of wavelet decomposition produces LL1, LH1, HL1, and HH1, where LL1 is the approximation matrix and LH1, HL1, HH1 are detail coefficients.
- 2nd level of wavelet decomposition (matrix LL1 is used) produces LL2, LH2, HL2, HH2.
- Diminish LL2 values using LL2 (i,j) <- LL2(i,j)/(m×n), where m and n are matrix dimension.
- Reverse the sign of the coefficient details matrices LH2<-LH2×-1, HL2<-HL2×-1, HH2<-HH2×-1, the reason behind performing the sign reverse operation is that the magnitude of the sinusoid corresponds to its contrast (the difference between the darkest and brightest peaks of the image).
- A negative magnitude represents contrast-reversal, i.e. the bright become dark, and vice-versa.
- Swap the contents of LL2 with HL2 and LH2 with HH2.
- Diminish LL1 values using LL2 (i,j) <- LL2(i,j)/(m×n).
- Reverse the sign of the coefficient details matrices –LH1, -HL2, -HH1.
- Swap the contents of LL1 with HL1 and LH1 with HH1.
- Apply the 2-levels Inverse wavelet transform.
- Encoded Image.

5. Decryption Algorithm

The decryption algorithm reveals the image's original details. This process is inverse of encryption process. The decoding process of the 1st wavelet decomposition is similar to that of the 2nd level. Thus, decoding the 1st level of the wavelet decomposition is achieved. In the last stage, the inverse discrete wavelet transform of the image is performed. The image frequencies are transformed back to the pixel domain, with the pixel values unaffected and the image details revealed. Using the proposed encryption/decryption algorithm, the decrypted image pixels will have the same values as the original image.

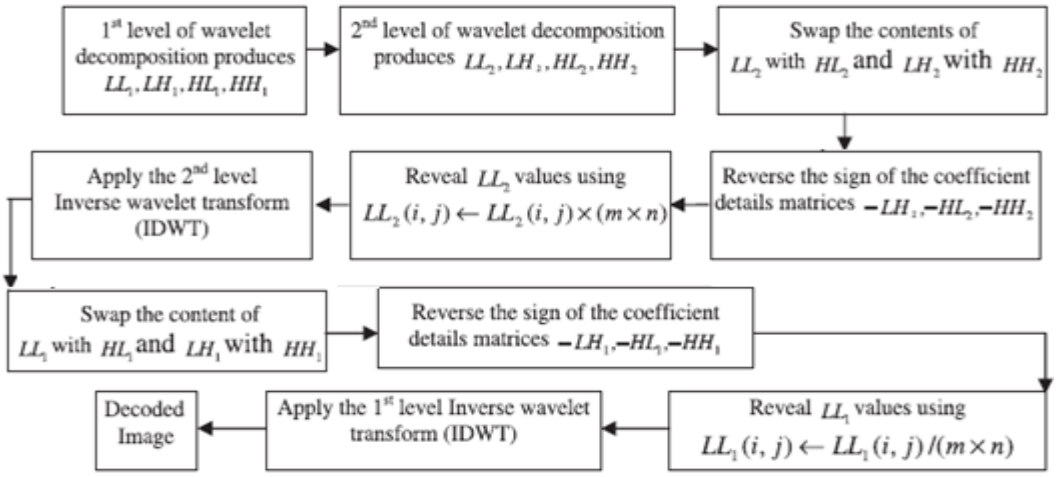

Figure: A flowchart of the proposed image decryption algorithm.

There are following steps of encryption algorithm:

- 1st level of wavelet decomposition produces LL1, LH1, HL1, and HH1, where LL1 is the approximation matrix and LH1, HL1, HH1 are detail coefficients.
- 2nd level of wavelet decomposition (matrix LL1 is used) produces LL2, LH2, HL2, HH2.
- Swap the contents of LL2 with HL2 and LH2 with HH2.
- Reverse the sign of the coefficient details matrices LH2<-LH2×-1, HL2<-HL2×-1, HH2<-HH2×-1.
- Reveal LL2 values using LL2 (i,j) <- LL2(i,j)×(m×n), where m and n are matrix dimension.
- Apply the 2-levels Inverse wavelet transform.
- Swap the contents of LL1 with HL1 and LH1 with HH1.
- Reverse the sign of the coefficient details matrices –LH1, -HL2, -HH1.
- Reveal LL1 values using LL2 (i,j) <- LL2(i,j)×(m×n).
- Apply the 1st level Inverse wavelet transform.
- Decoded Image.

6. Conclusion

Now a day's images play an important role in our lives, it is used in many applications. Therefore it is essential to protect the integrity and confidentiality of images. In this paper we presented survey of various image encryption techniques. Each technique having some advantages and disadvantages, so there is a need to design algorithm that reduce the correlation between the image pixels and increase the entropy so it is very difficult to decrypt by hacker. The proposed technique shuffles the image pixel position perfectly and changes the value of each pixel.

References

[1] Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform.
[2] Scalable Coding of Encrypted Images.
[3] A Novel Approach for Image Encryption using Dynamic SCAN Pattern
[4] An Image Encryption using Block based Transformation and Bit Rotation Technique
[5] The Haar–Wavelet Transform in Digital Image Processing