

## An efficient method for selective image encryption using wavelet transform for secure and fast communication

Ravikumar.K<sup>1</sup>, Shanmuga priya.G<sup>2</sup>

<sup>1</sup>Engineering Mathematics, Faculty of Engineering and Technology, Annamalai University, Annamalai Nagar, Tamil Nadu, India, 608002.

<sup>2</sup>Departments of Mathematics, Annamalai University, Annamalai Nagar, Tamil Nadu, India, 608002.

**Article History:** Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

**Abstract:** In this paper, we suggest a new formulation of selective partial encryption based on the Discrete Wavelet Transform (DWT) in order to verify an optimal and assured transmission and storage of images. This approach is faster since it permits a very important gain in the encryption-decryption processing time and more efficient because it allows to get an encrypted image.

**Keywords:** Discrete Wavelet Transform (DWT), Band Pass, Haar Wavelets, Image Encryption.

### 1. Introduction

The protection of digital image transmission has gained much attraction recently and many different methods for image encryption/decryption have been proposed. With the speedy improvement of internet and wide application of multimedia technology, people can communicate the digital multimedia information such as digital image, with others conveniently over the internet [1]. Image encryption has been really challenging than that of text encryption due to some inbuilt characteristic of images such as mass data capacity, high correlation among pixels and high redundancy. Fast (Efficient) image encryption has been an area of interest for research due to the need of real-time image encryption-decryption in various fields such as Military Image Transmission, Telemedicine and so on[2]. Telemedicine is evolving considerably due to the remarkable development of information and telecommunications technologies. This sector is based essentially on the exchange of medical information which is essentially images. This is due to the fact that medical imaging is currently considered to be the cross roads of all specializations since it is present in almost all medical records the development of techniques for securing the transmission and storage of medical images remains a necessity. To achieve this, one must resort to encryption and compression of images. Images will be transmitted via networks and/or stored in medical databases, they must be compressed in order to reduce transmission times, first, and second to improve the storage and archiving capacity on the other hand. In addition to that, in order to follow the laws of ethics and to eliminate any risk of disclosure, alteration or availability of any secrets concerning the patient's condition or professional secrets, the images must be encrypted before their transmission and storage[3].

Encryption is a process which facilitates the transmission of secret messages between two authorized end parties without any kind of interruption. Here the image which is to be communicated will be scrambled using the modified algorithm and the cipher image is transmitted to the receiver. Any encryption scheme uses a pseudo random value as a key to be shared with the receiver for the decryption process [4]. With an increase in transmission and distribution of digital image data through open natured wired or wireless IP networks, piracy operations have also increased. To restrain these activities, security of digital data is required at different stages of data archival, transmission and distribution [5]. Encryption is considered as the basic matter of defense in digital rights management security solutions. This provides data confidentiality and consequently prevents prohibited Copying and Distribution of valuable data. Application specific total or selective encryption method have been framed in different domains, with a major thrust on selective encryption that trade security for computational efficiency by encrypting only the most important part of multimedia data [6, 7].

### 2. Wavelet transform

Around 1980s a brand new mathematical instrument has been developed using wavelet transform. It is efficient for local analysis of non-stationary and fast transient wide band signals. The wavelet transform is a function of a time signal to the time scale joint representation, which is used in the short-time Fourier transform, the Wigner distribution and the ambiguity function. The impermanent aspect of the signals is preserved. The wavelet transform furnishes multi resolution analysis with dilated windows. The higher frequency analysis is done through narrower windows and the lower frequency analysis is done through wider windows. Thus, the wavelet transform is a constant- $Q$  analysis. The basic functions of the wavelet transform, the wavelets, are yield from a basic wavelet function by dilation and translation.

They satisfy an admissible condition so that the original signal can be reconstructed by the inverse wavelet transform. The wavelets satisfy also the regularity condition so that the wavelet coefficients decrease fast with the decreasing of the scale. The wavelet transform is local not only in time but also in frequency domain. To reduce the time–bandwidth product of the wavelet transform output, the discrete wavelet transform with discrete dilation and translation of the continuous wavelets can be used.

The orthonormal wavelet transform is implemented in the multiresolution signal analysis framework, which is based on the scaling functions. The discrete translates of the scaling functions form an orthonormal basis at each resolution level. The wavelet basis is generated from the scaling function basis. The two bases are mutually orthogonal at each resolution level. The scaling function is an averaging function. The orthogonal projection of a function onto the scaling function basis is an averaged approximation. The orthogonal projection onto the wavelet basis is the difference between two approximations at two adjacent resolution levels. Both the scaling functions and the wavelets satisfy the orthonormality conditions and the regularity conditions. The discrete orthonormal wavelet series decomposition and reconstruction are computed in the multiresolution analysis framework with recurring two discrete low-pass and high-pass filters, that are, in fact, the 2- band Para unitary perfect reconstruction quadrature mirror filters, developed in the sub band coding theory, with the additional regularity. The time–bandwidth product of the wavelet transform output is only slightly increased with respect to that of the signal. The wavelet transform is powerful tool for ultra-resolution local spectrum analysis of non-stationary signals, such as the sound, radar, sonar, seismic, electrocardiographic signals, and for image compression, image processing and pattern recognition. The wavelet transform can be easily generalized to any dimensions [8].

$$h_{jk}(x) = 2^{\frac{j}{2}} h(2^j x - k) \quad \text{--- (1)}$$

### 3. Discrete Wavelet Transform Based Image Decomposition

Wavelet transforms investigate the multi-scale structure of signal, which is important in signal processing and image compression. In digital image processing, the low-frequency component stand for the approximation and high-frequency details stand for detail information of an image [9]. Discrete wavelet transform (DWT) can analyze simultaneously an image in the time and frequency domains.

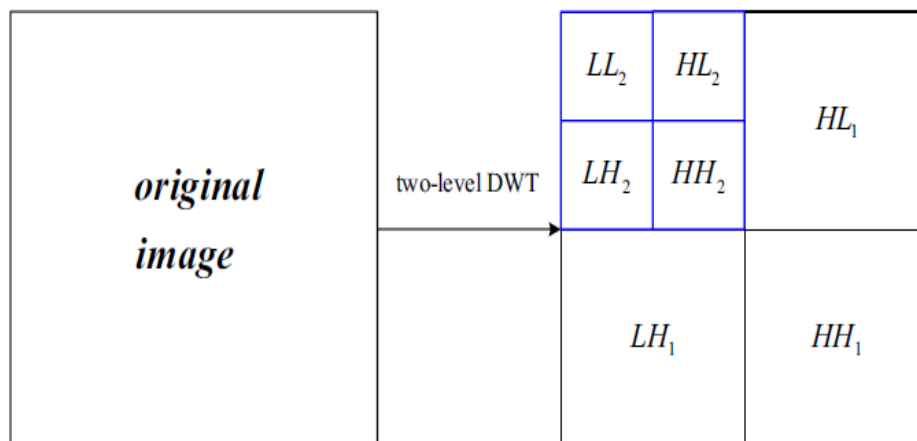
$$X[n] * h[n] = \sum_{k=-\infty}^{\infty} x[k].h[n - k] \quad \text{--- (2)}$$

Based on  $n$ -level DWT, an image can be decomposed into  $(3n + 1)$  sub-image: the low-frequency approximation ( $LL_n$ ) and  $3n$  high-frequency detail information:

$$HL_n, LH_n, HH_n, HL_{n-1}, LH_{n-1}, HH_{n-1}, \dots, HL_1, LH_1 \text{ and } HH_1 .$$

Thus, DWT has a multiresolution property that decomposes the images into multi-scale sub image [10].

Fig.1 illustrates the block diagram based on two-level DWT decomposition for a two-dimension digital image. Here in, the  $LL_2$  is the best approximation (i.e., the low-frequency component) of the original image in the DWT with the minimum scale and the minimum resolution. Other high-frequency sub images  $\{HL_2, LH_2, HH_2\}$  and  $\{HL_1, LH_1, HH_1\}$  are the detail information that corresponds to the edge, contour and texture of the image in different directions and resolutions.



**Figure 1.** Two level image decomposition based on DWT (2\*3+1)

Then the decomposition D for two-dimensional digital images based DWT and its inverse transform are defined as

$$D = WFW^T \quad \text{--- (3)}$$

$$F = (W)^{-1}D(W^T)^{-1} \quad \text{--- (4)}$$

Where,  $(W^T)$  denotes the transpose of matrix W and  $(W)^{-1}$  is the inverse matrix of W. By using DWT, an image can be diluted into any level sub-band images,

$$y_{high}[k] = \sum_n x[n].g[2k - n] \quad \text{--- (5)}$$

$$y_{low}[k] = \sum_n x[n].h[2k - n] \quad \text{--- (6)}$$

Where  $y_{high}[k] \rightarrow$ The Output of the high pass filters,  $y_{low}[k] \rightarrow$ The Output of the low pass filters

➤ LL: represents the data coming from two low-pass filters, one horizontal and the other vertical. The content of j corresponds to the original image but with a lower resolution.

➤ LH: represents data from two filters. The first is a horizontal low-pass, the other is high-pass vertical. Its content, therefore, corresponds to horizontal details.

➤ HL: represents data from two filters: a horizontal high pass and a vertical low pass. Its content, therefore, corresponds to vertical details.

➤ HH: this space undergoes a high-pass filtering in both directions; it then contains the diagonal detail information.

$$\varphi(x, y) = \varphi(x)\varphi(y) \quad \text{--- (7)}$$

And Scaling equation has

$$\varphi(x, y) = \sum_{m,n} h_{mn} \cdot 2\varphi(2x - m, 2y - n) \quad \text{--- (8)}$$

Since  $\varphi(x) \wedge \varphi(y)$  both Satisfy the Scaling equation

$$\varphi(x) = \sum_m h_m \cdot \sqrt{2}\varphi(2x - m) \quad \text{--- (9)}$$

We have  $h_{mn} = h_m h_n$

Thus two dimensional Scaling equation is Product of two one dimensional Scaling Equations.

#### 4. Methodology

##### 4.1 Encryption Algorithm

At the first step, Password will be created for encrypting the image. Text or special characters of the password will be used by the key generating algorithm a secret key will be generated. This generated key will not even know to the sender. Based on the key, encryption process will be carried out. In the beginning, wavelet transform will be chosen from the wavelet choosing function in the algorithm [11]. Haar, Daubechies and Symelet are possible wavelets.

The Haar Wavelet's mother wavelet function  $\Psi(t)$  can be

$$\Psi(t) = \begin{cases} 1, & \text{for } t \in \left[0, \frac{1}{2}\right), \\ -1, & \text{for } t \in \left[\frac{1}{2}, 1\right), \\ 0, & \text{otherwise.} \end{cases} \quad \text{--- (10)}$$

In Scaling Function  $\varphi(t)$  can be

$$\varphi(t) = \begin{cases} 1, & 0 \leq t < 1, \\ 0, & \text{otherwise.} \end{cases} \quad \text{--- (11)}$$

First step in wavelets produces four sub band matrixes for the given image.

XX  $\rightarrow$  low-low frequency sub band,

XY  $\rightarrow$  low-high frequency sub band,

YX  $\rightarrow$  high-low frequency sub band,

YY  $\rightarrow$  high-high frequency sub band.

Second step is decreasing the values of low-low frequency sub band by

XX (i,j)  $\rightarrow$  XX(i,j)/(m×n) ,Where m and n are the dimensions of the low-low frequency sub band.

Third step will be reversing the signs of XY, YX and YY sub bands, to inverse the magnitude of sinusoidal co-efficient. It will convert brighter side to darker side and darker side to brighter side.

Fourth and Fifth steps are the important process of this paper. Positions of the sub bands will be exchanged through three patterns,

1. Interchanging XX with YX and YX with YY.
2. Interchanging XX with XY and YX with YY.
3. Interchanging XX with YY and XY with YX.

On the Basis of the key, any one of the pattern will be chosen for interchanging the positions of sub bands. This process will be carried in two steps, in the first step, a pattern will be applied and in the second step, another pattern will be chosen for interchanging the positions of sub bands. Figure 2 explains the process of choosing wavelet mechanism and exchange of frequency sub bands. Now the Inverse Discrete Wavelet Transform (DWT) will be applied to produce the encrypted image. Thus the encrypted image and password will be shared only with the intended receiver [12].

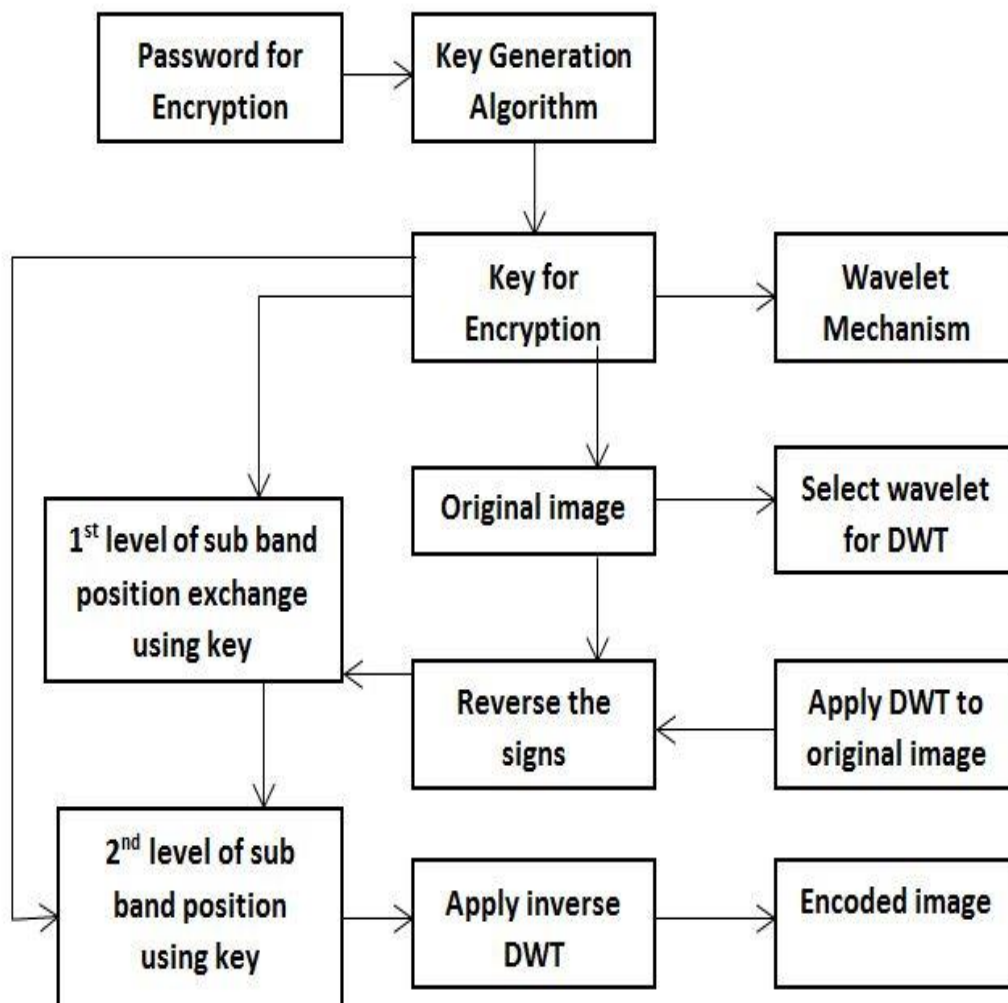


Figure 2. Flow Chart for Encryption Algorithm

#### 4.2 Decryption Algorithm

In the decryption algorithm, whole process will be reversed to generate the original image. Receiver will be prompted to enter the password for generating the decrypted image. If the password is same as the senders then the receiver will be permitted to decrypt the image; otherwise the process will be terminated. Similarly a key will be generated from the given password, and then Discrete Wavelet Transform (DWT) will be applied to the chosen wavelet. First step of the decryption will be second level of interchanging the sub band. Second step is interchanging the sub band as in the first level of encryption process. Now the values of XY, YX and YY will be inverse by multiplying (-1). During Encryption process, values of XX were lessened, now the same values will be

recreated through  $XX(i, j) \rightarrow XX(i, j) \times (m \times n)$ . Fig.3 indicates the decryption process. Finally, inverse wavelet transform will be applied to get the original image.

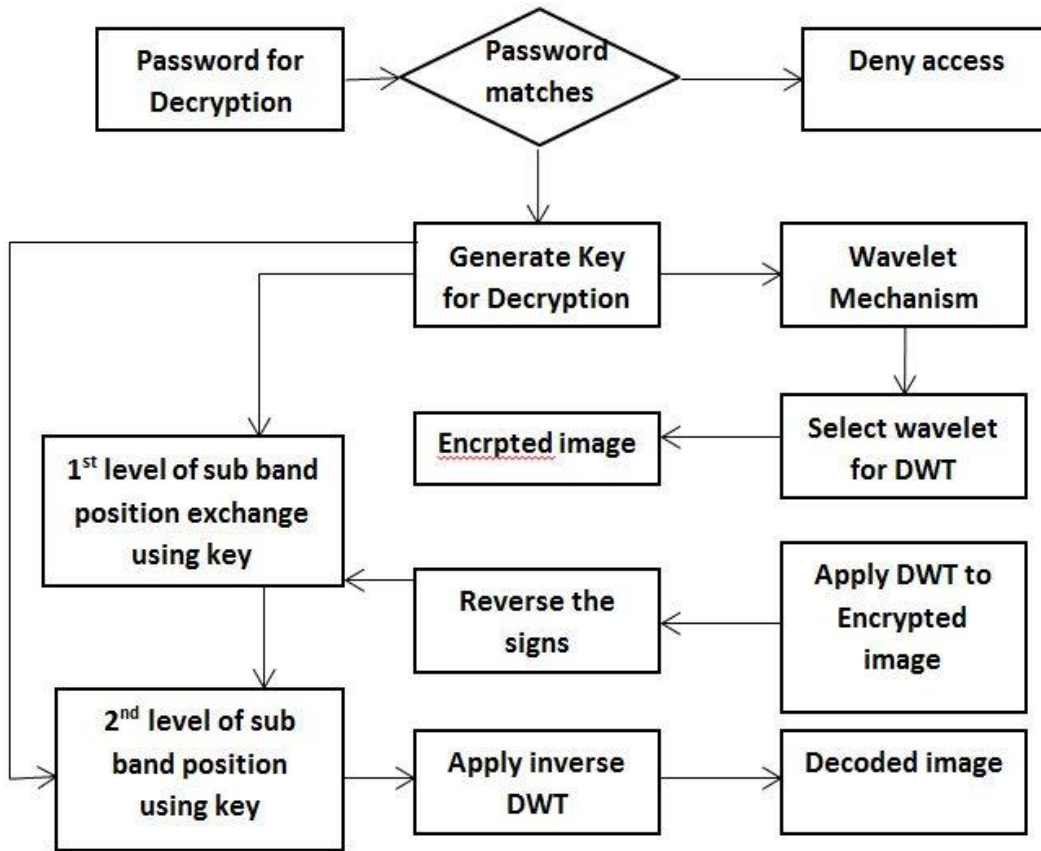


Figure 3. Flow Chart for Decryption Algorithm

5. Simulation results

For simulation purpose, simulation program was employed using MATLAB software. True color image for face recognition was chosen as shown in Figure.4.


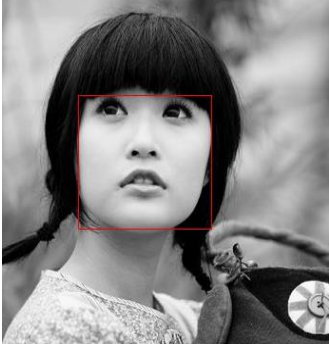




Figure 4. Original input image

The progress of face identification follows with converting the real image into black & white image for easy face identification as shown in Figure.5.1 and Figure.5.2. After the face has been recognized, the region of the face identified is encrypted by DWT using designed wavelet.

**5.1 Encryption and decryption process**


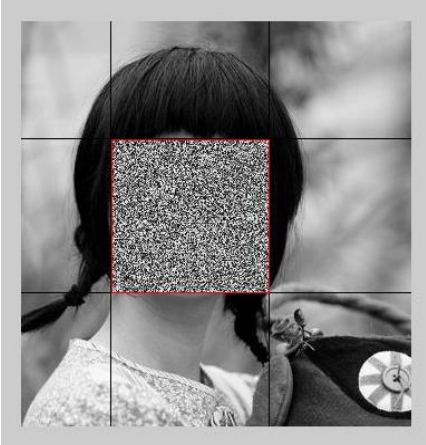


Encryption process includes the generation of key for safety data transformation. Figure.5.3 displays the encrypted image after four iteration using the keys. The mod operation should be applied for size of 225 to maintain gray scale value of encrypted image .Finally the encrypted part of the image will be added with the input image as shown in Figure.5.4.

	
<p><b>Figure 5.1-</b> Black &amp; white image of input colour image</p>	<p><b>Figure 5.2 -</b> Face identification</p>
	
<p><b>Figure 5.3 -</b> Encryption of face part (scrambling with dwt)</p>	<p><b>Figure 5.4 -</b> Encrypted face added with input image</p>

**Figure 5.** Encryption Process

In the decryption process, the key generated will be communicated to the receiver end secretly, which will ultimately yield the original image. Initially the encrypted image will be taken as the input for decryption process. Then the part of encrypted area will be identified. Decryption procedure will be done by using DWT upon successfully verification of the secret key. Finally the decrypted area will be included in the image which yields

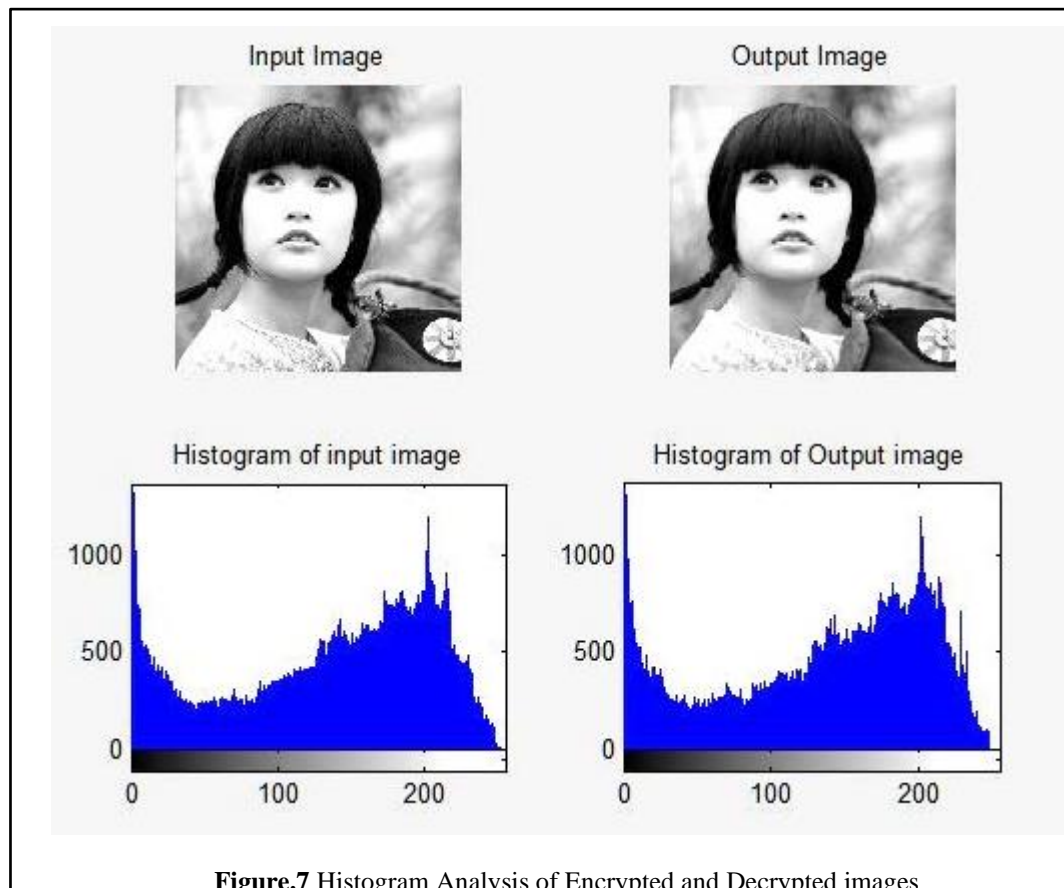
the original true image at the receiver end as shown in steps in Figure.6. This process is much secured and data transmission will be definitely fast when compared with the reported results.

	
<p><b>Figure 6.1-</b> Encrypted image taken as input for decryption</p>	<p><b>Figure 6.2-</b> Encryption area identification</p>
	
<p><b>Figure 6.3-</b> Encryption area segmented</p>	<p><b>Figure 6.4-</b> Decryption done (using DWT) and added with image to produce original image</p>

**Figure 6.** Decryption Process

**5.2 Histogram analysis**

Histogram is a graphical and approximate representation of the distribution of numerical data. Image histogram will plot the number of pixels for each tone value. Here the histogram for both the original and encrypted image is shown in Fig.7. The encrypted image has relatively equal distributed pixels, with the original distribution is clearly distributed. The maximum pixel value in original value and encrypted value is ~1400.



## 6. Conclusion

In this paper, we have suggested a novel method for transmitting the images with selective encryption of the face and decryption of the same at receiver end. The technique used here results in a significant reduction in encryption and decryption time. The goal of this paper is to obtain an effective cipher and high-quality image compression to achieve both security against unauthorized access during data transmission through an unsecured channel and high compression to allow for a low transmission rate. For the encryption and compression, we used the wavelet transformation, and the results were highly satisfactory; this method allowed us to achieve a perfect reconstruction. The new crypt-compression approach presented in this work is effective since it makes it possible to prevent any attempt at correct diagnosis from the image. Thus, our next work is to explore a better way to further improve the performance of quantum image encryption algorithm for group of faces in single image using wavelet transforms.

## References

1. Alattar, Adnan & Alregib, Ghassan & Al-Semari, Saud. (1999). Improved selective encryption techniques for secure transmission of MPEG video bit-streams. *IEEE International Conference on Image Processing*. 4. 256 - 260 vol.4. 10.1109/ICIP.1999.819590.
2. Abdmouleh, Mohamed & Khalfallah, Ali & Bouhlel, Med. (2017). A Novel Selective Encryption DWT-Based Algorithm for Medical Images. 79-84. 10.1109/CGiV.2017.10.
3. Pommer, Andreas & Uhl, Andreas. (2003). Selective encryption of wavelet-packet encoded image data: Efficiency and security. *Multimedia Syst...* 9. 279-287. 10.1007/s00530-003-0099-y.
4. Subashanthini, S. & Cherukuri, Aswani Kumar & Muthukumar, Pounambal. (2020). Image Encryption Using New Chaotic Map Algorithm. 10.1007/978-3-030-16660-1\_45.
5. Al-ma'adeed, Somaya & Al-Ali, Afnan & Abdalla, Turki. (2012). A New Chaos-Based Image-Encryption and Compression Algorithm. *Journal of Electrical and Computer Engineering*. 2012. 10.1155/2012/179693.
6. Taneja, Nidhi & Raman, Balasubramanian & Gupta, Indra. (2011). Selective image encryption in fractional wavelet domain. *Aeu-international Journal of Electronics and Communications - AEU-INT J ELECTRON COMMUN*. 65. 338-344. 10.1016/j.aeu.2010.04.011.



7. Sharma, Prerana& Mishra, Devesh&Agarwal, Ankur. (2012). Efficient image encryption and decryption using discrete wavelet transform and fractional Fourier transform. Proceedings of the 5th International Conference on Security of Information and Networks, SIN'12. 153-157. 10.1145/2388576.2388598.
8. Shakir, Haidar. (2019). An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling. Multimedia Tools and Applications. 78. 10.1007/s11042-019-07766-z.
9. Parthasarathy, M. &Srinivasan, B.. (2015). Increased Security in Image Cryptography using Wavelet Transforms. Indian Journal of Science and Technology. 8. 10.17485/ijst/2015/v8i12/62433.
10. Hu, Wen-Wen & Zhou, Ri-Gui&Luo, Jia& Jiang, Shexiang&Luo, Gao-Feng. (2020). Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. Quantum Information Processing. 19. 10.1007/s11128-020-2579-9.
11. Butt, Khushbu& Li, Guohui& Khan, Sajid&Manzoor, Sohaib. (2020). Fast and Efficient Image Encryption Algorithm Based on Modular Addition and SPD. Entropy. 22. 112. 10.3390/e22010112.
12. Alsaedi, Mohammed. (2020). Novel Scheme for Image Encryption and Decryption Based on a Hermite-Gaussian Matrix. 10.1007/978-3-030-17795-9\_16.