An Efficient Data Hiding Technique in Frequency domain by using Fresnelet Basis

Muhammad Nazeer and Dai-Gyoung Kim*

Abstract—A novel method for an efficient data hiding is proposed with more robust retrieving hidden information against various attacks. The proposed method employs the data encryption by appropriate handling of Fresnelet transform for hiding signature information. Different patterns of signatures data are presented for testing the validity of the method. A quantitative evaluation of the quality of extracted signatures is carried out with the correlation function. Also it is analyzed through experiments how the proposed method is effective against the cropping, blurring, sharpened, brightness, Gaussian noise and JPEG compression. Furthermore, the proposed model has the flexibility in using large size of data hiding information as well as supports the multi-frequency domains such as wavelet transform domain for a safe data transmission.

Index Terms—Encryption, Decryption, Information Data hiding, Fresnelet transform, Wavelet transform.

I. INTRODUCTION

Secure data communication has sundry importance in current era of advanced technology. The primary tactic was to shielded communications by means of data encryption. In recent years, cryptography is an engrained field, repetitively purported of as an art chocked with influences of adroit mathematicians. Cryptography contemplates on manipulative techniques to map the original information to scramble at sender end, and at the receiver side to decrypt it [1]. Information smacking, on the supplementary hand, states to a variegated class of problems where safe information is carried out by smacking a significance message in specific host data. Though, this system was previously measured by ancient Greeks. The main reasons that directed researchers to drone in this concern are enormous application of Internet communications. Above and beyond, the fabricated production of such hypermedia can easily attacked by some hackers or pirates. In this regard, internet users recurrently need to communicate the private information. The public way to organize this is to transform the information into an encrypted structure. The subsequent information can be extracted only by those who have a proper keys or method to get its original form. A most weakness to encryption is that the presence of information is not concealed properly.

Manuscript received March 27, 2012; revised April 19, 2012. This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (NRF-2011-0026245). The travel grant for attending the conference was supported by the Higher Education Commission (HEC) H-9 Islamabad (Pakistan).

Nazeer Muhammad: Division of Applied Mathematics, ERICA, Hanyang University, Ansan, 426-791; South Korea (e-mail: nazeer@hanyang.ac.kr).

Dai-Gyoung Kim*: (Corresponding Author) Division of Applied Mathematics, ERICA, Hanyang University, Ansan, 426-791, South Korea, (phone: 031-400-5458; fax: 031-416-5460; e-mail: dgkim@hanyang.ac.kr).

Information that has been encrypted, even though unintelligible, still exists as a kind of some trivial data. With an opportunity of an adequate time, somebody could eventually unencrypt the concealed information. An answer to this offending is steganography. It is an ancient skill of hiding messages so that they are not detectable, based upon no transformation or permutation. The hidden communication is plain, but unsuspicious to the third party. Steganography's firm is to hide the communication, while cryptography scrambles a meaning so that it cannot be explicit. Even if someone knows the existence of the communication, he cannot recover the clear message if he does not know the appropriate keys. This method offers improved security for fast and secure transformation than traditional approaches. On the other hand, data can be hide into a common host object, but if someone extracts it: he/she can also get the information easily. Therefore, our idea is to apply both of them: eventually in case one gets the embedded stuff: he/she will face an encrypted data.

In this script, we propose an algorithm: the efficient Data Hiding Technique in Frequency domain by using Fresnelet transform. Liebling et al. [2] have adopted a family of wavelet like basis functions named as Fresnelets.

The transformation depends on the distance parameter to the transform plane. This suggests that the applications of the Fresnelets transform to digital data hiding can be more flexible than the method using only the Fresnel transform [3], [4], [5] and [6] or with the wavelet multi-resolution analysis [7]. It is important that, even if the attacker detect the information and also know the embedding algorithm, but still it is impossible for understanding the clear data without the Fresnelets coefficient keys in the form of distance and sampling interval In nut shell, it is a technique for image compression along with cryptography as well.

It not only improves the encryption strength with immense information but also gives better compression and faster transmission at a larger network domain. Furthermore, due to its wavelet multi-resolution coefficients, this method has better resistance to conservational attacks than other methods in frequency domain embedding. The paper is ordered as follows. Theoretical expression of an efficient data hiding technique by using Fresnelets coefficients in the cognitive of mathematical expressions describes in the section 2. Section 3 presents simulation results to evaluate this new Algorithm and section IV of this paper presents the conclusion.

II. THEORETICAL EXPRESSION

The Fresnelet transform is a transform appearing in connection with Fresnelet diffraction of the waves. This
numerical Fresnelet transform has been used for numerical image reconstruction from Fresnelet transform hologram at the long wave-length region [2]. The Fresnelet transform bases functions are shift invariant on a level- by-level compression.

For the numerical expression of Fresnelet transform the multi-resolution properties of Fresnel transform and wavelet are being to be considered. It is sufficient to numerically carry out simulation of the diffraction phenomena of the waves. Hence, only unidirectional Fresnel transforms needs to be carried out [4] and [5]. Inverse transform to numerically restore the original data rigorously with forward and inverse transformations is not a significant problem.

Let us use the unitary Fresnel transform of a function as the convolution integral model is shown in Fig. 1:

\[
\tilde{f}_\tau(x) = (f \ast k_\tau)(x) \quad \text{for } \tau > 0 \text{ and } \tau = \sqrt{\pi z}
\]  

(1)

where \( \tilde{f}_\tau \) is a Fresnel transform of a function \( f \in L_2(\mathbb{R}) \) using tilde; where \( \tau \) is a scaling factor and \( z \) is a distance factor as stated by Eq. (1) between the object and observing planes and a wavelength \( \lambda \). \( M \) shows the number of an elements in an array.

\[
k_\tau(x) = \frac{1}{\tau} \exp \left( i\pi \left( \frac{x^2}{\tau^2} \right) \right), \quad \text{for } \tau > 0.
\]

(2)

where \( k_\tau \) is the kernel of convolution operator, whereas the Fresnel transform for the given function \( f(t) \) expressed as

\[
\tilde{f}_\tau(x) = \frac{1}{\tau} \int f(t) \exp \left( -i\frac{1}{\tau} \right) \left( \frac{x-t}{\tau} \right)^2 dt.
\]

(3)

Next, it is assumed that the distance \( z \) from the source plane to the observation plane is much larger, so that the following approximation holds known as 1-D Fresnel approximation Eq. (3). The wave field in the range where this approximation is valid is the one caused by Fresnel diffraction. This is achieved by 3-FFT algorithm and leads to the spatial convolution with respect to the function along with the Fresnel impulse response \( h(x) \) of a function, expressed as

\[
h(x) = \frac{dt}{\tau} \exp \left( i\pi \left( \frac{V^2}{\tau^2} \right) \right).
\]

(5)

where \( V \) is the spatial frequency in 1-D Fresnel transform and phase function \( h(x) \) act as a propagator. Furthermore, the constant phase term in the original Fresnel diffraction field is emitted in Eq. (4) by employing the convolution theorem: that lead to unitary magnification. To inverse the function at the point of the object wave front has been back propagated as

\[
f(x) = \left( \tilde{f}_\tau \ast k_\tau \right)(x), \quad \text{where } f \in L_2(\mathbb{R}).
\]

(6)

where inverse Fresnel kernel is defined by

\[
k_\tau(x) = \frac{1}{\tau} \exp \left( -i\pi \left( \frac{x^2}{\tau^2} \right) \right).
\]

(7)

According to Fresnel transform properties, we will be able to consider one dimensional Fresnel Transform and simply extend the results to two dimensions by using separable basis functions. The unitary two dimensional \( \tilde{x} = (x, y) \), Fresnel transform can be expressed as a 2-D convolution integral by employing Eq. (6) and Eq. (7).

\[
\tilde{f}_\tau(x, y) = f \ast k_\tau(x, y).
\]

(8)

for \( \tau > 0 \in L_2(\mathbb{R}^2) \) and following the Fresnel transform properties, we have the separable kernel:

\[
k_\tau(x, y) = \frac{1}{\tau^2} \exp \left( i\pi \left( \frac{1}{\tau^2} \right) \right) = k_\tau(x)k_\tau(y)
\]

(9)

Fresnelets are the Fresnel transforms of the standard wavelet transform with same generating function at each scale. We considered the \( h \) and \( g \) being high and low pass filter of Haar wavelet transform for generating the Fresnelets coefficients:

\[
h = [h_\nu, h_\eta] = \left[ \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right] \quad \text{and} \quad g = [g_\nu, g_\eta] = \left[ \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right].
\]

Two Parameter families for Haar wavelet function \( (\psi_{j,k})_t \):

\[
(\psi_{j,k})_t(x) = 2^{j/2} \psi \left( 2^j x - k \right)
\]

(10)

where \( j, k \in \mathbb{Z} \) with \( 2^{j/2} \) is scaling factor. Fresnelet transform of Haar wavelet function \( (\tilde{\psi}_{j,k})_t \) generated the
low pass filter dilation equation \((\tilde{\phi})_\tau\), by using low pass filter of Haar wavelet in (10):

\[(\tilde{\phi})^n_{j,k} = k \ast \psi^n_{j,k} \] leads to \((\tilde{\psi})^n_{j,k}(x) = 2^{j/2}\tilde{\phi}^n_{j/2,2^{j-k}}(2^j x - k),\)

\[(\tilde{\psi})^n_\tau(x) = g_0(\tilde{\psi}_{1,0})_\tau(x) + g_1(\tilde{\psi}_{1,1})_\tau(x),\]

\[(\tilde{\psi})^n_\tau(x) = \frac{1}{\sqrt{2}}(\tilde{\psi}_{1,0})_\tau(x) - \frac{1}{\sqrt{2}}(\tilde{\psi}_{1,1})_\tau(x),\]

\[(\tilde{\psi})_\tau(x) = (\tilde{\psi}_{1,0})_\tau(2x) - (\tilde{\psi}_{1,1})_\tau(2x-1).\] (11)

To generate the high pass filter dilation equation for scaling function \((\tilde{\phi})_\tau\), by using high pass filter of Haar wavelet: we consider the multiresolution Analysis of detail space \(V_j\):

\[V_j = \text{span} \left\{ \phi(2^j t + 1), \phi(2^j t), \ldots \right\} \cap L^2(\mathbb{R}).\]

\[V_j = \text{span} \left\{ \phi(2^j t - 1) \right\} \cap L^2(\mathbb{R}).\] (12)

An orthonormal basis for \(V_j\) is the set \(\{\phi_{n,k}(x)\}\) where \(j, k \in \mathbb{Z}\). Projectoin function from \(L_2(\mathbb{R})\) into \(V_j\) space w.r.t. Fresnel transform in Eq. (10) to Eq. (12) by employing the value of \(h\):

\[(\tilde{\phi})^n_{j,k} = k \ast \phi^n_{j,k} \] leads to \((\tilde{\phi})^n_{j,k}(x) = 2^{j/2}\tilde{\phi}^n_{j/2,2^{j-k}}(2^j x - k),\)

\[(\tilde{\phi})_\tau(x) = h_0(\tilde{\phi}_{1,0})_\tau(x) + h_1(\tilde{\phi}_{1,1})_\tau(x),\]

\[(\tilde{\phi})_\tau(x) = (\tilde{\phi}_{1,1})_\tau(2x) + (\tilde{\phi}_{1,1})_\tau(2x-1),\]

\[(\tilde{\phi})_\tau(x) = \frac{1}{\sqrt{2}}(\tilde{\phi}_{n,0})_\tau(x) + \frac{1}{\sqrt{2}}(\tilde{\phi}_{n,1})_\tau(x).\] (13)

Hence, we got the Fresnel coefficient w.r.t Haar Wavelet Function \((\tilde{\phi})_\tau\) and Haar scaling function \((\tilde{\phi})_\tau\) in Eq. (11) and Eq. (13) respectively:

\[LL = \tilde{U}(x, y) \ast \left[ \tilde{\phi}^n_{\tau} (x) \tilde{\phi}^n_{\tau} (y) \right].\] (14)

where Fresnellet Haar wavelet high coefficient details are:

\[HL = \tilde{U}(x, y) \ast \left[ \tilde{\phi}^n_{\tau} (x) \tilde{\phi}^n_{\tau} (y) \right],\]

\[LH = \tilde{U}(x, y) \ast \left[ \tilde{\phi}^n_{\tau} (x) \tilde{\phi}^n_{\tau} (y) \right].\] (15)

where \(\tilde{U}_{\tau}(x, y)\) is a two dimensional (an image) Fresnel transform of data hiding. To compress this data: the \(LL\) (approximation detail) of scale 1 has to be decomposed at second level: i.e., \(LL_2\) (approximation detail), \(HL_2\) (horizontal detail), \(LH_2\) (vertical detail), \(HH_2\) (diagonal detail) sub bands by critically subsampling horizontal and vertical channels using sub band filters. For sake of imperceptibility, the \(HL_1, LH_1, HH_1, HL_2, LH_2\) and \(HH_2\) finest scale Fresnellet coefficient retained by owner. To get the following coarser scaled Fresnellet coefficients, the sub band \(LL_1\) (approximation detail), is further decomposed and subsampled critically. The process is repeated up to two levels, which is attained by the application at hand: and explained in Fig. 2. In reconstruction process, it is called the inverse Fresnellet transform.

On the flow chart shown in Fig. 2 and Fig. 3, we determine the encryption (compressed) of information data for embedding purpose in host image. Compression is important for space intensive data hiding. The discrete Fresnellet transform is effective for decomposition of large size data information. Usually original image is transformed and structured information data is embedded in frequency domain. Where, the distance or sampling interval can be used as keys. By using these keys with inverse of Fresnellet Coefficient with respect to Haar wavelet; we can decrypt (reconstruct) the compressed information from embedded image.

A. An Embedding Process

In proposed method, the size of host image and information image is same: \(m \times m\) at the first. By applying Fresnellet transform to information data, the compressed size \(n \times n\) has been achieved. where, \(m = 2 \ast p \ast n\) (\(p\) is +ve integer) has been satisfied the sufficient condition to embed both real and imaginary data of Fresnellet transform. In proposed scripts, we consider the algorithm with the condition \(m = 4n\) \((p=2)\), whereas embedding calculation formula can be derive as

\[\tilde{F}_\tau = \text{fresnellet}(f, d),\]

where \(\tilde{F}_\tau \in (\tilde{F}_\tau, LL_1, \tilde{F}_\tau, HL_1,\tilde{F}_\tau, LH_1,\tilde{F}_\tau, HH_1)\), considering

\[\tilde{F}_\tau \in (\tilde{F}_\tau, LL_1)\] which leads to \(\tilde{F}_\tau = \text{fresnellet}(\tilde{F}_\tau, d)\).

Whereas \(\tilde{F}_\tau' \in (\tilde{F}_\tau', LL_2, \tilde{F}_\tau', HL_2,\tilde{F}_\tau', LH_2,\tilde{F}_\tau', HH_2)\), and

\[\tilde{F}_\tau' \in (\tilde{F}_\tau', LL_2).\] Moreover, the \(\tilde{F}_\tau' \in (R_{non}, I_{non})\)
construct \( P_{2n,n} \in (R_{scw} - \bar{R}, I_{scw} - \bar{I}) \) and determine the

\[
E_{embedding} = H_{image} + w \ast PNR \times SVD(\mathbb{I}_{data})
\]  

(17)

where, \( d_1,d_2 \): both distance are considered as a key parameter, \( f \): Information data, \( \bar{f} \): Fresnelet Transform of information data, \( \tilde{f} \): first level Fresnelet approximation \( \tilde{f} \): second level Fresnelet approximation, \( R,I \): real and imaginary parts of information image, \( \bar{R},\bar{I} \): averages of real and imaginary parts of data image, \( P_{2n,n} \): embedding data block of information image. \( \mathbb{I}_{data} \): compressed data of information image, \( H_{image} \): host image, \( E_{embedding} \): embedded image. \( SVD \): Singular Value Decomposition

For embedding purpose, we use compressed form \((m/4 \times m/4)\) of information data by considering sub-band LL2 of Fresnelet transformed as shown in Fig. 2 as well as in Fig. 3 by following Eq. (14).

\[
\begin{array}{c}
\text{LL1} \quad \text{HL1} \\
\text{LH1} \quad \text{HH1} \\
\end{array}
\quad \rightarrow
\begin{array}{c}
\text{LL2} \quad \text{HL2} \\
\text{LH2} \quad \text{HH2} \\
\end{array}
\]

Fig.2. Fresnelet bases decomposition setup

Furthermore, it is important to hide a digital information data into the host (cover) image in situations where only the real number data are treated. For this reason, we decompose the Fresnelet transformed (complex numbers) data into real and imaginary parts. By using these parts, we further construct the compressed coded pattern of information data. Furthermore, in first level decomposition of discrete wavelet transform of host image and compressed coded watermark (CCW) are embedded into the respective sub-bands by using the singular valued decomposition (SVD) algorithm [9].

\[
\begin{align*}
\text{LL2} & \rightarrow \text{HL2} \\
\text{LH2} & \rightarrow \text{HH2} \\
\end{align*}
\]

Fig.3. the Embedding flow chart

B. An Extraction Process

In order to extract the embedded data, the one level wavelet coefficients of host Lena image is subtracted from respective coefficients of the information embedded image. Resultant information image are undergone to the process of inverse SVD. Whereas, the inverse Fresnelet transform reconstruct the information data identity image.

\[
I\tilde{f} = \text{ifresnelet}(I\tilde{f}, d_j), \quad \text{leads to } I\tilde{f} \in (f).
\]

(20)

where \( I\tilde{f} \): inverse Fresnelet Transform of information data, \( I\tilde{f} \): inverse of second level Fresnelet approximation \( \mathbb{I}'_{data} \): compressed data of information image, \( inv(PNR) \): inverse Pseudo noise random generator

III. SIMULATION AND EVALUATION

To analyze the algorithm, MATLAB simulation has been performed for embedding and extraction of information data image. Different experiments are performed on embedded data to validate the robustness of proposed method. Image processing tricks like filtering, cropping, compression, geometric transformations has applied on information data. Quality of extracted information data is examined with respect to original information data with correlation (CORR) factor shown in Eq. (22) by means of MATLAB (Image Processing Toolbox). Where, a number between 0 and 1 to specify a confidence level: between two images.

\[
\text{CORR} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (u_{ij} - \bar{u}) (v_{ij} - \bar{v})}{\sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} (u_{ij} - \bar{u})^2 \sum_{i=1}^{M} \sum_{j=1}^{N} (v_{ij} - \bar{v})^2}}
\]

(21)

where \( \bar{u} = \text{mean2}(u), \) and \( \bar{v} = \text{mean2}(v) \) are averages of embedded and extracted images. Whereas, a modified PSNR (Peak Signal Noise Ratio) technique [8]: has been
used to assess the quality of embedded image by the proposed information data hiding method. It is simply defined through mean-squared error (MSE) shown in Eq. (22). Whereas, $\lambda$ is introduced for reducing MSE to minimum value defined as in Eq. (25) as follows:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left\| u(x,y) - v(x',y') \right\|^2$$  \hspace{1cm} (22)

$$\lambda = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left\| u(x,y) - v(x',y') \right\|^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left\| u(x',y') \right\|^2}$$  \hspace{1cm} (23)

$$PSNR = 10 \times \log_{10} \left( \frac{MAX^2}{MSE} \right)$$  \hspace{1cm} (24)

where $k, l, m$ and $n$ are integers with ranges to maximum value of $M$ (column of image) and $N$ (row of image). The bigger the value of $PSNR$, better the imperceptibility. For our simulation and evaluation, we consider the following four gray scale images of same sizes, $512 \times 512$.

Fig. 5. (a) is an host image for information data hiding and (b) to (c) the signature image 1 (S1), signature image 2 (S2) and signature image 3 (S3) are data information images for hidden transmission.

Fig. 6. The EMB (Embedded Image) for three signature images S1, S2 and S3 with $PSNR$ are carried out in (a), (b) and (c) with Eq. (25). ICD (Information Coded Data) and IRD (Information Reconstruction Data) are analyzed for $COR$ with Eq. (22).

A. Robustness against Compression

Test of JPEG compression is performed to evaluate the robustness of algorithm contrary to lossy compression. Then the quality of embedding information data is compressed with public compression free online software [10]. As shown in Fig. 7, the quality of compressed data purely depends on the quality ratio of compression. As increase in compression ratio decrease the quality of extracted information image.

B. Robustness against Image Cropping

In addition to the image compression discussed above, there is cropping attack in which a part of the image is sliced out. Here, advantages of the Fresnelet transform method against cropping attack are briefly discussed. Image cropping is performed on information data by cropping 25% and 75% of image respectively. At that point the extraction algorithm is performed on this cropped image. And robustness against cropping is verified by applying changed percentage. It is observed that the quality of extracted data image endure very well till 75%~80% as shown in Fig.8.
Fig. 8. (a1) to (c2) are the effect of image cropping at 25%, whereas (a3) to (c4) are the effect of image cropping at 75% of original data.

C. Robustness against Filtering

Filtering is a major application of image processing that is used to remove the noise of different varieties. Gaussian filters are significant in numerous signal and image processing applications. Gaussian filters are considered by low overshoots, narrow bandwidths and sharp cutoffs. The filtered images are shown in Fig. 9.

Fig. 9. (a1), (b1) and (c1) are effect of Gaussian filtering at level 3, whereas (a2), (b2) and (c2) are effect of Gaussian filtering at level 5.

D. Robustness against Rotation

The transformations with modify angle of orientation are recognized as rotation. In this case, the method is weak against rotation attack due to application of Fresnelet coefficient for decryption of encrypted information data: based on the Haar wavelet filter as shown in Fig. 10. However, an application of Fresnelet coefficients for B-splines or Mexican hat wavelet filters due to their symmetry nature: for development against rotation attack is a topic for future study.

IV. Conclusion

Our proposed technique needs less memory space of host media and have fast transmission rate because image decomposition technique is applied by dwindling the original information data. Moreover, it is possible to embed information data in various noticeable planes with different distance keys of Fresnel transform. In nut shell, all kinds of image data such as letter, shape and photo can be embed as an information image. The application of this method does not only hide the transmitted data but also encrypt it, for resistance to leakage the vibrant information.

REFERENCES