Cryptography Based Image Encryption by Secure Reversible Data Hiding Technique

Kammari Kalyani (M. Tech scholar) [1],
Dr. P. Abdul Khayum, **M. Tech, Ph. D** (Professor of ECE) [2]
Department of Electronics & Communication Engineering[1,2]
G. PULLAREDDY Engineering College (Autonomous), Kurnool, Andhra Pradesh-518007, India[1,2]
kammarikalyani902@gmail.com[1], abdkhayum@rediffmail.com[2]

ABSTRACT

In this paper we are proposing novel reversible image data hiding scheme by using encrypted domain. Embedding of information can be done by using public key modulation process; here there is no need to access the secret encrypted key. Two-class SVM classifier is used at the decoder side to separate the encrypted and non-encrypted images. And we can decode the embedded message and original signal. Compared to the conventional methods the proposed work is going to give the high embedding capacity and the original image and embedded message is going to be reconstructed perfectly. By seeing the experimental results we can conclude that SVM is giving better results.

Key Words— Feature extraction, reversible image data hiding (RIDH), signal processing over encrypted domain, SVM.

I. INTRODUCTION

A. Basics of Image Data Hiding

Reversible image information hiding (RIDH) is a distinct category of knowledge hiding procedure, which ensures ideal reconstruction of the duvet snapshot upon the extraction of the embedded message. The reversibility makes such an photograph knowledge hiding strategy exceptionally attractive within the crucial scenarios, e.g., army and remote sensing, scientific picture sharing, regulation forensics, and copyright authentication, the place high fidelity of the reconstructed cover snapshot is required. The vast majority of the existing RIDH algorithms are designed over the plaintext area, namely, the message bits are embedded into the customary unencrypted pix compress targeted snapshot facets, to vacate room for message embedding.

B. Data Hiding most important terms and Notions

Among the many lossless procedures of information embedding there are two common domains of operation: spatial and frequency. Spatial methods are characterized by using the embedding of messages into the least massive bits (LSBs) of photograph pixels, whilst in frequency ways the message is embedded after a targeted develop into is performed by means of enhancing frequency coefficients of the quilt photograph.

Recently, the study on signal processing over encrypted domain has won increasing awareness, exceptionally pushed with the aid of the desires from cloud computing platforms and more than a few privacy-retaining functions. This has brought about the investigation of embedding extra information within the encrypted pics in a reversible trend. In many useful situations, e.g., at ease far off sensing and cloud computing, the parties who process the photo information are un-trusted. To defend the privacy and safety, all portraits might be encrypted before being forwarded to a un-trusted third party for further processing. For example, in comfy remote sensing, the satellite images, upon being captured by means of on-board cameras, are encrypted, and then sent to the base station(s), as proven in Fig. 1. After receiving the encrypted pix, the bottom station embeds a confidential message, e.g., base station identification, area knowledge, time of arrival, nearby temperature, wind pace, etc, into the encrypted portraits.

II. LITERATURE SURVEY

J. Tian, "Reversible knowledge embedding using a difference growth"

In this paper, we've got provided a easy and efficient reversible date-embedding process for digital pictures. We explored the redundancy in the digital content to attain reversibility. Each the payload capability limit and the visible pleasant of embedded portraits are among the many first-rate in the literature.

Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, Reversible knowledge hiding

A novel reversible data hiding algorithm, which can get well the customary image with none distortion from the marked picture after the hidden information had been extracted, is provided in this paper. This algorithm utilizes the zero or the minimal points of the histogram of an photograph and rather modifies the pixel grayscale values to embed information into the photograph. It may embed more knowledge than most of the present reversible information hiding algorithms.

III. PROPOSED METHOD

A. RIDH Scheme over Encrypted Domain

As a substitute of due to the fact that committed encryption algorithms tailored to the scenario of encrypted-area data hiding, we here stick with the conventional circulate cipher applied in the typical format. That is, the cipher text is generated through bitwise XOR using the plaintext with the important thing circulation. If not in any other case distinctive, the commonly used movement cipher AES in the CTR mode (AES-CTR) is assumed.

Flowchart of the proposed work is given below,

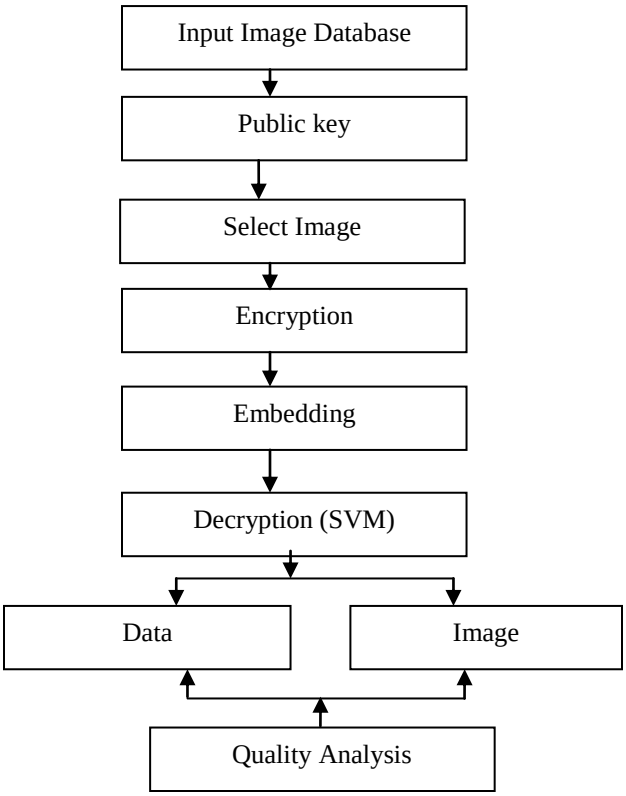

Fig.1 Flow Chart of Proposed System

The ensuing data hiding paradigm over encrypted area would be extra almost valuable since of two explanations.

1) Move cipher used in the average format (e.g., AES-CTR) is still probably the most preferred and secure encryption tools, because of its provable safety and high software/hardware implementation affectivity. It is probably not easy, and even infeasible, to influence consumers to adopt new encryption algorithms that have not been utterly evaluated.

2) massive amounts of information have already been encrypted utilizing move cipher in a general means. When move cipher is employed, the encrypted image is generated by

$$[[f]] = Enc(f, K) = f \oplus K \qquad (1)$$

Where f and [[f]] denote the long-established and the encrypted pix, respectively. Here, K denotes the important thing circulate generated utilizing the secret encryption key K . In this paper, without lack of generality, the entire snap shots are assumed to be 8 bits. During this paper, we use [[x]] to represent the encrypted variation of x. Clearly, the common photograph can be got via performing the following decryption function:

$$f = Dec([[f]], K) = [[f]] \oplus K. \qquad (2)$$

As mentioned previous, the encrypted photograph [[f]] now serves as the cover to accommodate message to be hidden. We first divide [[f]] into a series of non overlapping blocks $[[f]]^{i's}$ of dimension M × N, where i is the block index. Each block is designed to hold n bits of message. Letting the quantity of blocks within the image be B, the embedding ability of our proposed scheme becomes n • B bits. To permit efficient embedding, we advise to use S = 2n binary public keys Q_0, Q_1,..., Q_{s-1}, each of which is of size L = M × N × eight bits. All Q j 's, for zero ≤ j ≤ S − 1, are made publicly obtainable, which implies that even the attacker knows them. These public keys are preselected prior to the message embedding, in step with a criterion of maximizing the minimal Hamming distance amongst all keys. The algorithm developed by way of MacDonald can be utilized to this end.

Notice that all of the public keys are constructed into the information hider and the recipient when the whole method is installed, and for this reason, it is not crucial to transmit them during the information embedding stage. Also, for constant S and L, Hamming confirmed that an higher bound on the minimum Hamming distance can accept as follows. First, examine two integers m_1 and m_2 by using m1

$$\sum_{i=0}^{m1} \binom{L}{i} \le \frac{2^L}{S} < \sum_{i=0}^{m1+1} \binom{L}{i} \quad (3)$$

$$\sum_{i=0}^{m2} \binom{L-1}{i} \le \frac{2^{L-1}}{s} < \sum_{i=0}^{m2+1} \binom{L-1}{i} \qquad (4)$$

Where, L i = (L!/i!(L − i)!).

It can be shown that both m1 and m2 are unique. Then, the minimum Hamming distance among all Q j 's satisfies

$$d_{min} \le \max\{2m1 + 1, 2m2 + 2\}. \qquad (5)$$

The schematic diagram of the proposed message embedding algorithm over encrypted area is shown in Fig. 2. In this paper, we do not remember the case of embedding more than one watermark for one single block, meaning that each and every block is processed once at most. For simplicity, we expect that the quantity of message bits to be embedded is n • A, where A ≤ B and B is the quantity of blocks inside the image.

The steps for performing the message embedding are summarized as follows.

Step 1: Initialize block index i = 1.

Step 2: Extract n bits of message to be embedded, denoted by W_i.

Step three: in finding the general public key $Q_{[Wi]d}$ associated with W_i, the place the index $[W_i]d$ is the decimal illustration of W_i . For example, when n = three and W_i = 010, the corresponding public secret is Q_2.

Step 4: Embed the length-n message bits W_i into the ith block by way of

$$[[f]]_i^{\omega} = [[f]]_i \oplus Q_{[w_i]_d} \qquad (6)$$

Step 5: Increment i = i + 1 and repeat Steps 2–4 except all the message bits are inserted. The watermark length parameter A desires to be transmitted on my own with the embedded message bits. There are numerous ways to clear up this drawback.

For instance, the present non separable RIDH schemes upon trivial changes, can still make sure embedding safety even if the data hiding secret is eliminated, if we repair the way in which of partitioning a block into S0 and S1 (specifically, do not use knowledge hiding key to randomize the block partitioning), then an attacker nonetheless can't compute the fluctuation operate [18, eq. (10)] so as to decode the embedded message. This is considering the fact that an attacker does no longer access to the secret encryption key k. In different words, the safety mechanism in the encrypted domain will also be naturally expanded to provide safety for message embedding, putting off the need of introducing one more knowledge hiding key.

Moreover to deciding on this property, we, in section VI, will exploit the message in distinguish capacity to show that the removing of knowledge hiding key will not hurt the embedding protection. Before providing the data extraction and photo decryption methods, let us first investigate the facets that can be used to discriminate encrypted and no encrypted picture blocks. The classifier designed consistent with these aspects might be shown to be primary within the proposed joint information extraction and snapshot decryption method.

B. Feature Resolution for Discriminating Encrypted and Non-encrypted photo Blocks

To differentiate encrypted and customary unencrypted picture blocks, we here design a feature vector ρ = (H, σ, V), integrating the traits from multiple views. Right here, H is a tailor-made entropy indicator, σ is the SD of the block, and V represents the directional neighborhood complexities in four directions. The formation of the above feature factors will likely be designated as follows. When put next with the fashioned unencrypted block, the pixels in the encrypted block tend to have a much more uniform distribution. This motivates us to introduce the neighborhood entropy into the characteristic vector to capture such individual characteristics.

However, we need to be cautious when calculating the entropy values on the grounds that the number of on hand samples in a block can be rather restricted, leading to estimation bias, especially when the block dimension is small. For instance, within the case that M = N = eight, we most effective have 64 pixel samples, whilst the range of each and every sample is from 0 to 255. To curb the negative influence of inadequate quantity of samples relative to the large variety of every pattern, we advise to compute the entropy variety established on quantized samples, the place the quantization step dimension is designed based on the block measurement. In particular, we first follow uniform scalar quantization to each and every pixel of the block

$$f^{\wedge} = \left[\frac{MN.f}{256}\right] \qquad (7)$$

Where f and f` denote the common and the quantized pixel values, respectively. Undoubtedly, f` falls into the range [0, M N − 1]. The entropy indicator H founded on quantized samples is then given through

$$H = -\sum_{j=0}^{MN-1} p(j) l0g\ p(j) \qquad (8)$$

Where p(j) is the empirical chance of j within the quantized block. As a single first-order entropy quantity is probably not adequate to duvet the entire underlying characteristics of a block, we endorse

augmenting the characteristic vector with the aid of introducing a further element, i.e., the SD outlined by using

$$\sigma = \sqrt{\frac{1}{MN}\sum_{j}(f(j)-\mu)^2} \qquad (9)$$

the place f(j) is the jth pixel in the block and μ = (1/M N) j f(j) is the pattern imply over the entire samples within the block. Via together with this option detail, we are able to strengthen the classification performance as the data depressiveness and denseness will also be better mirrored.

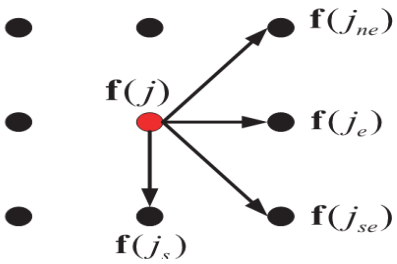

Fig.2 Illustration of the neighbors of f(j).

In addition to the above feature components, we also include directional complexity indicators that encode the local geometric information. To this end, we define a four-tuple vector V = (v1,v2,v3,v4), where

$$\upsilon_1 = \sum_{j}|f(j)-f(j_{ne})|$$

$$\upsilon_2 = \sum_{j}|f(j)-f(j_e)|$$

$$\upsilon_3 = \sum_{j}|f(j)-f(j_{se})|$$

$$\upsilon_4 = \sum_{j}|f(j)-f(j_s)| \qquad (10)$$

where f(j_{ne}), f(j_e), f(j_{se}), and f(j_s) represent the neighbors in the 45° (northeast), 0° (east), −45° (southeast), and −90° (south) directions, relative to f(j), as shown in Fig. 2. Upon the determination of the feature vector ρ, we train a two-class SVM classifier with RBF (Gaussian) kernel [29] taking the for

$$Ker(X_i, X_j) = e^{-\gamma\|x_i - x_j\|} \qquad (11)$$

The zero-class and 1-class correspond to the unencrypted and encrypted photo blocks, respectively. Here, the learning image set contains one hundred images of dimension 512×512, with a broad form of traits including average scenes, artificial snap shots, synthetic images, and textual images. The offline trained SVM classifier will probably be used to discriminate the encrypted and non-encrypted photograph patches within the method of information extraction and photograph decryption.

C. Joint Data Extraction and Picture Decryption

The decoder within the data core has the decryption key k and makes an attempt to recover both the embedded message and the long-established photograph at the same time from $[[f]]^w$, which is assumed to be flawlessly got without any distortions. Word that this assumption is made in just about the entire existing RIDH methods. As a result of the interchangeable property of XOR operations, the decoder first XORs $[[f]]^w$ with the encryption key movement ok and obtains

$$f^{\omega} = [[f]]^{\omega} \oplus K. \qquad (12)$$

The resulting f^w is then partitioned into a series of non overlapping blocks $f_i^{w's}$ of size M × N, similar to the operation conducted at the embedding stage. From (6), we have

$$f_i^{\omega} = f_i \oplus Q_{[W_i]_d} \qquad (13)$$

The joint knowledge extraction and photo decryption now turns into a blind sign separation trouble as both W_i and f_i are unknowns. Our approach of fixing this main issue is founded on the following statement: f_i, because the common photo block, in all probability displays detailed picture structure, conveying semantic information. Be aware that $Q_{[Wi]d}$ ought to

in shape probably the most elements in Q = Q0, Q_1,..., Q_{S-1}. Then, if we XOR f_i^w with all Q_j's, one of the results must be f_i, which might reveal structural know-how. As will grow to be clear shortly, the other outcome corresponds to randomized blocks, which will also be individual from the customary structured f_i. Extra particularly, we first create S decoding candidates with the aid of XOR ing f_i^w with all of the S viable public keys

$$f_i^{(0)} = f_i^{\omega} \oplus Q_0 = f_i \oplus Q_{[W_i]_d} \oplus Q_0$$

$$f_i^{(0)} = f_i^{\omega} \oplus Q_1 = f_i \oplus Q_{[W_i]d} \oplus Q_1$$

$$f_i^{(S-1)} = f_i^{\omega} \oplus Q_{s-1} = f_i \oplus Q_{[W_i]d} \oplus Q_{s-1} \quad (14)$$

As mentioned earlier, one of the above S candidates must be f_i, while the others can be written in the form

$$f_i^{(t)} = f_i \oplus Q_{[W_i]d} \oplus Q_t \quad (15)$$

the place, t = [Wi]d. The outcome $f_i^{(t)}$ = Enc(f_i, $Q_{[Wi]d} \oplus Q_t$) corresponds to an encrypted variant of f_i with equivalent key circulation being $Q_{[Wi]d} \oplus Q_t$. Be aware that the entire public keys Q_j's, for zero ≤ j ≤ S − 1, are designed to have maximized minimum Hamming distance, and the higher bound is given in (5). For this reason, $f_i^{(t)}$ tends to lose the picture structural information, making it appear random. To identify which candidate corresponds to f_i, we follow the designed two-classification SVM classifier to these S candidates. Let r = (r_0, r_1,..., r_{S-1})be the vector recording the classification outcome, the place r_j = 0 and r_j = 1 correspond to the original (structured) and randomized blocks, respectively. If there exists a particular j such that r_j = 0, then we decode the embedded message bits as

$$W_i = [j]_2 \quad (16)$$

where [j]$_2$ denotes the length-n binary representation of j and n = log2 S. For example, if n = 3 and j = 7, then [j]$_2$ = 111. Upon determining W_i , the original image block can be easily recovered by

$$f_i = f_i^w \oplus Q_{[W_i]d} \quad (17)$$

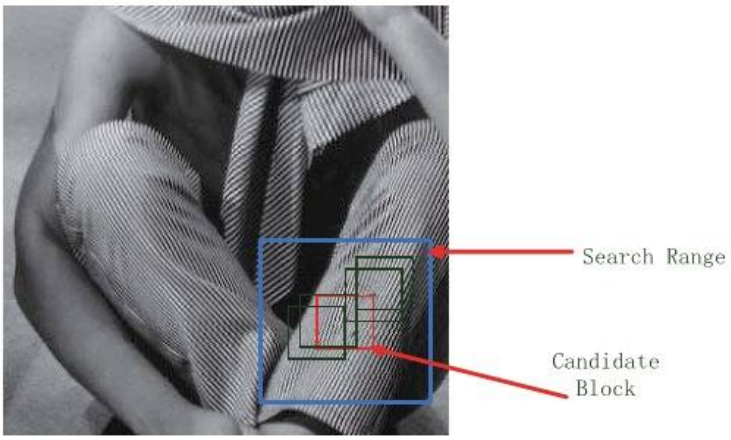

Fig.3 Illustration of the error correction mechanism based on image self similarity.

Nonetheless, we do notice a few circumstances the place there exist a couple of j's or no j such that r_j = 0. When any of these two instances happens, it indicates that some decoding errors show up.

To formally analyze these error and later propose an mighty error correction mechanism, we define two types of classification mistakes.

1) Type I Error: $fi^{(j)} = f_i$, while r_j = 1.

2) Type II Error: $f_i^{(j)} = f_i$, while r_j = 0.

Form I error almost always happens when the normal block fi is very elaborate, e.g., from incredibly textured regions, behaving similarly as an encrypted block. Variety II error regularly arises when the block size is rather small, making an encrypted block mistakenly be categorized as an long-established unencrypted one. As validated experimentally from 200 scan photos of size 512 × 512, for a designated block, we anticipate that at most one form of error will occur. Beneath this assumption, both sort I and kind II mistakes can be conveniently detected.

Even for those incredibly textured pictures, it's discovered that similar blocks would be determined in a nonlocal window [30], as additionally shown in Fig. Four. In step with this phenomenon, the proposed error correction method is headquartered on the next key commentary: if a block is appropriately decoded, then with very high probability, there are some equivalent patches around it. This sort of property of nonlocal photograph similarity motivates us to rank the entire abilities candidate blocks in step with the minimal distance with the patches in a nonlocal search window. To this finish, we first outline a to-be-corrected set C via

$$C = \begin{cases} \left\{ f_i^{(j)} I \; 0 \le j \le s-1 \right\} & Type\ I\ error\ detected \\ \left\{ f_i^{(j)} I \; r_j = 0 \right\} & Type\ I\ error\ detected \end{cases} \quad (19)$$

Variety I error detected type II error detected. (19) For any candidate block $f_i^{(j)}$ in C, we calculate its 2 distances from all of the different blocks in a search variety $D\backslash\{f_i^{(j)}\}$, the place D shares the equal center as $f_i^{(j)}$ and its dimension is experimentally decided as 5M × 5N. We then can compute the minimal patch distance inside the hunt window

$$d_i^{(j)} = \min_{D \in D \backslash f_i^{(j)}} \left\| f_i^{(j)} - D \right\|^2 \quad (20)$$

The place D is an arbitrary block of measurement M × N inside $D\backslash f_i^{(j)}$. Here, we hire the straightforward MSE criterion when ranking the candidate blocks. Through including the feel course and scale into the above minimization framework, we could extra strengthen the error correcting performance, however we find that the further attain is as a substitute restricted and the incurred complexity is giant. The candidate $f_i^{(j)}$ that gives the smallest $d_i^{(j)}$ is then selected because the decoded block.

Assume that the encryption is performed without destroying the constitution of JPEG bit flow. For instance, the encryption scheme proposed in can be utilized to this finish. We can XOR the encrypted parts with some of the designed S binary public keys, in step with the message bits to be embedded. On the extraction stage, we try all of the S potentialities and establish the one that generates structured snapshot patches in the pixel area. The embedded message can then be extracted based on the index of the identified public key.

Protection analysis

According to the context of the assault, the attacker could have access to special amounts of expertise. Naturally, the attacker as a minimum can entry to watermarked sign, specifically, $[[f]]^w$. In some events, the embedded message or the quilt sign will also be on hand to the attacker [31]. Accordingly, the security degree of the encrypted-area RIDH scheme should be assessed for distinctive contexts. Just like the drawback of evaluating the protection for encryption primitives, Cayre defined three forms of attacks.

1) The watermarked most effective attack (WOA), in which the attacker simplest has entry to watermarked portraits.

2) The recognized message attack, where the attacker has entry to a couple of pairs of previously watermarked pix and the related messages. Without doubt, the presently transmitted message bits aren't known to the attacker.

3) The recognized normal assault, where the attacker has access to a couple of pairs of earlier watermarked pics and the corresponding quilt photo. Surely, the current quilt photo will not be identified to the attacker. As defined in [31], the needs of the final two assaults are more often than not to recover the data hiding key, as a way to extract the long run embedded messages or hack distinctive portions of content material watermarked with the same key.

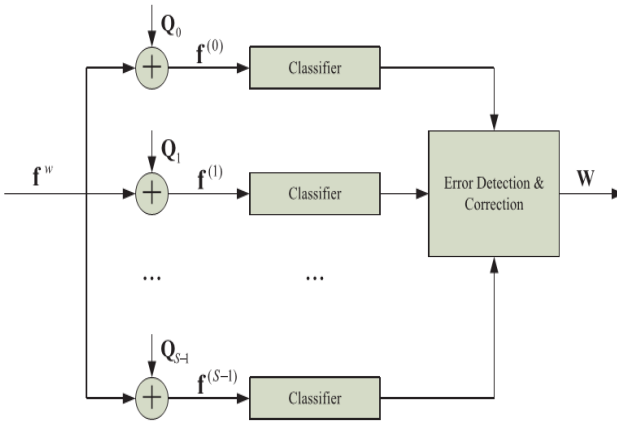

Fig.4 Schematic of the data extraction.

In our proposed RIDH scheme, the information hiding key has been eliminated, and for that reason, these two attack units usually are not relevant. Underneath the WOA, the one assault sort relevant to our scheme, the attacker attempts to extract the embedded message and/or get well the customary photograph from the watermarked and encrypted photo $[[f]]^w$. Before evaluating the security beneath WOA, allow us to first give the definition of message indistinguishability, which must preserve for any comfy encryption system. Definition of Message Indistinguishability—Concrete variant [32]:

We say that an encryption scheme (Enc, Dec) is (c,) message indistinguishable if for every two messages G and G, and for each Boolean perform T of complexity no bigger than c, now we have

$$\left|P\left[T\left(Enc(K,G)\right)=1\right]-P\left[T\left(Enc(K,G')\right)=1\right]\right| \leq \epsilon \quad (21)$$

The place, the chance is taken over the randomness of Enc() and the alternative of k . The message indistinguishability implies that the attacker can do no higher than easy random guessing if he simplest observes the cipher textual content. This property is regarded as a general requirement for any cozy encryption scheme. We then have the following theorem involving the safety of our RIDH algorithm.

Theorem 1: Assuming that the encryption scheme (Enc, Dec) is secure in terms of message indistinguishability, then our RIDH process is relaxed under WOA assault. Sketch of the Proof: once you have the watermarked and encrypted snapshot $[[f]]^w$, we can nonetheless partition it into non overlapping blocks of measurement M × N. For every block, we can generate S decoding candidates in a similar fashion as (14)

$$f_i^{(0)} = [[f]]_i^w \oplus Q_0 = [[f]]_i^w \oplus Q_0 \oplus K_i = Enc(f_i^w \oplus Q_0 \oplus K_i)$$

$$f_i^{(1)} = [[f]]_i^w \oplus Q_1 = [[f]]_i^w \oplus Q_1 \oplus K_i = Enc(f_i^w \oplus Q_1 \oplus K_i)$$

$$f_i^{(S-1)} = [[f]]_i^w \oplus Q_{s-1} = [[f]]_i^w \oplus Q_{s-1} \oplus K_i = Enc(f_i^w \oplus Q_{s-1} \oplus K_i) \quad (22)$$

Where, K_i denotes the sub key flow for the i^{th} block. With any discovered $f_i^{(j)}$, it is computationally infeasible to figure out, with likelihood drastically higher than 1/S, which one among $f_i^w \oplus Q_0$, $f_i^w \oplus Q_1$, . . . , $f_i^w \oplus Q_{S-1}$ is the message encrypted by Ki, due to the property of message indistinguishability described in (21). For this reason, the attacker making an attempt to extract the embedded message bits from [[f]]w should be equipped to do no higher than random guessing. This proves the protection of our proposed encrypted-domain RIDH technique against WOA attack.

IV. RESULTS

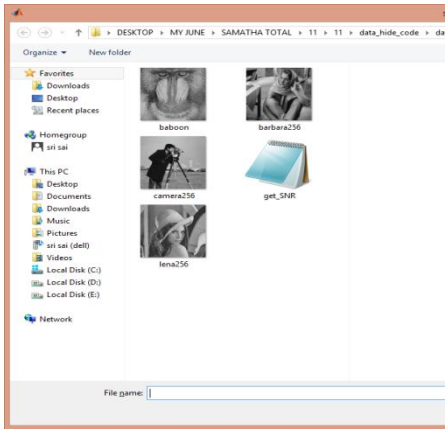

Fig.4.1 select an input image

There is a chance to select image for user from given image data base so for selected image will calculate the parameters

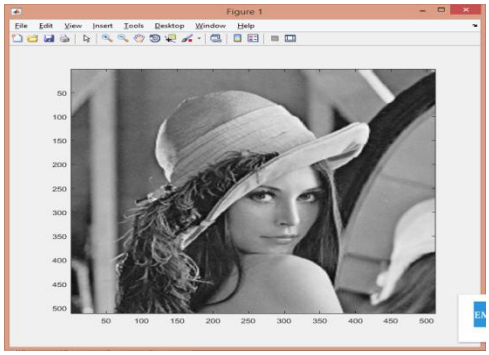

fig.4. 2 Input image selected by the user

lena.bmp image is selected for proposed implementation.and all the parameters are calculated for these leno.bmp

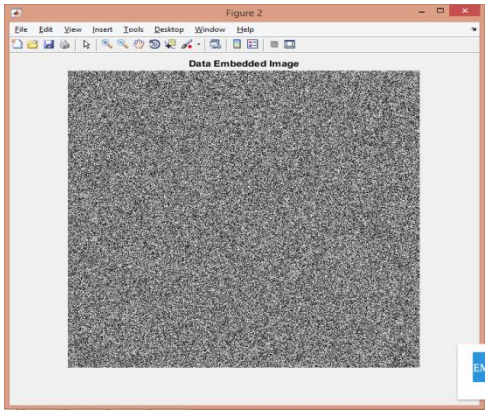

Fig.4.3 Data embedded image after encryption.

First we will apply public key cryptography and after that we will embed the data.

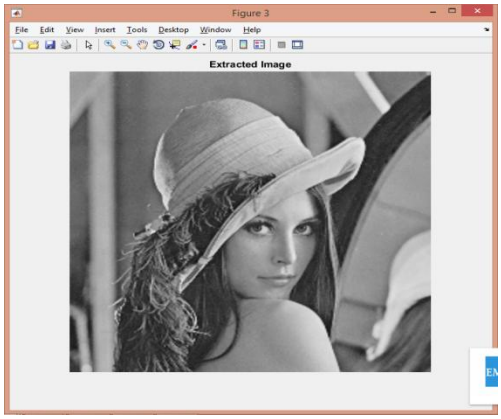

Fig.4.4 Extracted image

Finally with the help of SVM classifier we extracted data as well as image.

PERFORMANCE PARAMETRS FOR DIFFERENT IMAGES(PROPOSED[SVM])

Images	PSNR	ERROR	ACCURACY	CAPACITY
Lena.bmp	27.29	0	100	16384
Baboon.bmp	27.4730	0	100	16384
Cameraman.bmp	27.4566	0	100	16384
Barbara.bmp	26.8461	0	100	16384

Elapsed time is 27.3284 seconds.

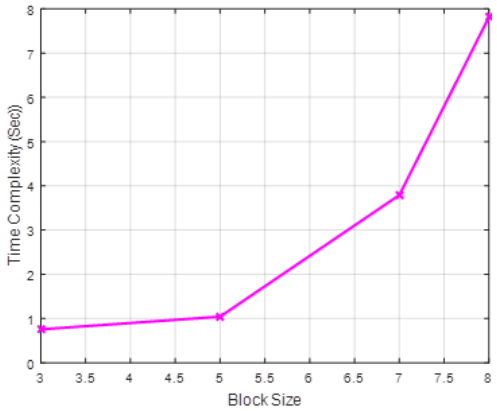

Fig.4 Block size vs. time complexity

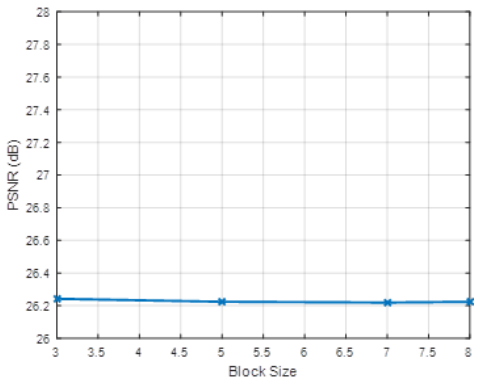

Fig.4 Block size vs. PSNR

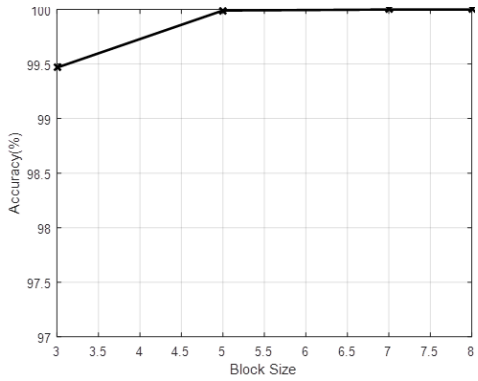

Fig.4 Block size vs. accuracy

CONCLUSION

In this paper for the encryption process we are using RIDH method and the modulation can be done by public key. So no need to use any secret encrypt key and we can embed the information by using the XOR operations. in the side of decryption we are using Two-class SVM classifier to divide the encrypted and decrypted image. The proposed experimental results giving better results compared to the previous methods. The SVM classifier is giving high efficiency.

REFERENCES

[1] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005. [2] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless watermarking for image authentication: A new framework and an implementation," IEEE Trans. Image Process., vol. 15, no. 4, pp. 1042–1049, Apr. 2006.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[4] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1091–1100, Jul. 2013.

[5] C. Qin, C.-C.Chang, Y.-H.Huang, and L.-T. Liao, "An inpaintingassisted reversible steganographic scheme using a histogram shifting mechanism," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 7, pp. 1109–1118, Jul. 2013.

[6] W.-L. Tai, C.-M.Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 6, pp. 906–910, Jun. 2009.

[7] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[8] Y. Hu, H.-K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 2, pp. 250–260, Feb. 2009.