International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Encryption and Watermarking of Remote Sensing Images for Crop Insurance

Abhima Prasad[1], Dr. Vishwanath N[2], Dr. Sreela Sreedhar[3], Saira Varghese[4]

[1]*PG Student, Dept. Computer Science Engineering, Toc H Institute of Science and Technology, Kerala*
[2]*Professor, Dept. Computer Science Engineering, Toc H Institute of Science and Technology, Kerala*
[3]*Assoc.Professor & HOD, Dept. Computer Science Engineering, Toc H Institute of Science and Technology, Kerala*
[4]*Asst.Professor, Dept. Computer Science Engineering, Toc H Institute of Science and Technology, Kerala*

Abstract - *Remote sensing is most widely used technology in crop insurance. Agricultural Insurance is one of the methods by which the farmer can stabilize farm income and invest and guard against losses due to many natural disasters Remote sensing images contain a lot of information and so they are vulnerable to loss, theft or interception due to storage in the cloud or the transmission through public channel. In the existing system, farmer himself has to upload the image to the system and sometimes they manipulate the image to get more claims. It will be very difficult for insurer to come and physically verify damage claim in order to give insurance to many farmers. This system makes use of It will be very difficult for insurer to come and physically verify damage claim in order to give insurance to many farmers this system makes remote sensing technologies for crop loss assessment.*

The proposed framework is designed for the farmer's in order to claim for crop insurance. The image acquisition center would remotely collect the images of crop damage. The farmers could request for the images of their agricultural fields which got affected to natural hazards. The image acquisition center watermark the image and send it to the farmer, so the farmer can check whether they provide the correct image of destructed area. Then image acquisition center would encrypt the image and send to the insurance company. Hence the insurance company will be receiving a watermarked image from farmer and also an encrypted image from the image acquisition center. The insurance company would decrypt the image and extract the watermark sequence in order to check whether any tamper detection has been occurred

Key Words: **Authentication, Encryption, DNA Encoding, Henon Map, Watermark Embedding, Tamper Detection**

1. INTRODUCTION

Remote sensing is the acquisition of information about an object or phenomenon without making any physical contact.it has a wide range of applications include forestry, photography, mining and many more. But in the field of agriculture, the remote sensing technology plays a significant role.[1]-[6]There are wide range of applications of remote sensing in the agricultural sector [7]-[9].Remote sensing images are highly sensitive as they contain a lot of visual information. Remote sensing snap shots of touchy regions are prone to loss, robbery or interception because of garage with inside the cloud or the transmission via public channel. Image encryption and watermarking provides a technical way to prevent information leakage and authenticity. Encryption schemes like advanced encryption standard AES [10], elliptic curve cryptography have been proposed for encrypting the images. However these technologies are not suitable for remote sensing images due to redundancy, high pixel correlation, and bi-dimensionality etc. To solve this problems the proposed framework, design a novel remote sensing image encryption scheme based on DNA coding, DNA bases probability along with a watermarking protocol for tamper detection.

Cryptography and watermarking have similar application. Watermarking is more robust. A robust watermark should survive a variety of attacks such as image cropping, modification, or other image processing techniques. Basically there are three types of watermark [34]:

1. Fragile watermark is the most sensitive watermark. Any changes made to the image can be easily detected by fragile watermark. It is mostly used for tamper detection in images.
2. Semi-fragile watermark has higher robustness than fragile Watermark but it can resist only some kind of image transformation. One of the most common applications of semi-fragile watermark is used to detect malignant transformations.
3. Robust watermark can resist most of the transformations and it is the most popular watermark and is widely used in the applications. Robust watermark is used in tamper detection applications.

One of the main purposes of watermarking the image is to avoid manipulation of image by users and to detect tamper in the image. The watermarking as well as DNA cryptography have a wide range of applications in medical fields, remote sensing projects and so on.. The remote sensing technology can be widely used in the agricultural field for so many interesting reasons. The primary application of remote sensing in agriculture include identifying crop conditions, increasing precision in farming,

determining moisture content of soil, crop production forecasting, determining crop damage and crop progress, crop identification, crop condition analysis and stress detection, drought monitoring, water content determination of the field crop and Crop health analysis. Among them, the most application is the crop insurance scheme making use of remote sensing images. Agriculture can be easily impacted by natural events and disasters like flood, earthquakes, fire, hailstorm etc.as the agriculture relies on the weather, climate, and water availability to thrive. Crop insurance aims to provide a comprehensive insurance cover against failure of the crop due to natural hazards thus help in stabilizing the income of the farmers. In the earlier system, farmer himself has to upload the image to the system and sometimes they manipulate the image to get more claims from the insurance company. It will be very difficult for loss assessors to come and physically verify damage claim. So in order to avoid that it can make use of remote sensing images as it contain all the information.

2. RELATED WORK

Remote sensing images have a significant role in the field of agriculture. The remote sensing images contain a lot of visual information so they have to be encrypted it in order to prevent information leakage. Chaotic maps are promising a new direction for image encryption when compared with the conventional encryption schemes [9]-[12].Basically the chaos system have several characteristic's like it's high sensitivity towards the initial condition determinacy, ergodicity and so on. The sequences produced by the chaotic system are often pseudo random sequences which are very complex and difficult to be analyzed and predicted. All these properties are exploited in the field of image processing techniques, mainly for encryption. Permutation Diffusion Structure (PDS) is widely in chaos based cryptography as the typical ciphers based on chaotic maps are partioned in to two stages that is permutation and diffusion[13].An excellent image encryption algorithm combined with chaotic system provides high randomness and sensitivity to the plain image and security key. Mandal et al.[14] designed a lightweight image encryption scheme based on DNA computing and chaos system. Encryption method used is one dimensional logistic map for key generation along with DNA coding to get the cipher images. In [16],Gunavati et al designed satellite image encryption based on RC4 encryption algorithm which is not a best way to encrypt images. Ashraf et al analyzed the features of Henon map such as its high sensitivity to initial conditions, fast computational speed. Minute variations in the initial point of the Henon map will lead to major changes and different behavior which is well suitable for cryptography. Similarly the cryptosystem based on DNA computing [17]-[20] have several interesting features like massive parallelism and ultra-power consumption. Zhang et al[20] exploited the features of Lorentz system along with DNA encoding operations for image encryption. According to DNA encoding all the pixel values in the plain image will be converted in the form of DNA sequence according to the DNA rules, that is to decompose the color image into grey scale image so that each pixel will be having an 8 bit value. The 8 bit grey value is converted into 4 DNA codes according to the DNA encoding rules so as to reduce the time complexity for the encryption.

And then the encoded plain image is operated with DNA operation rule in order to get the final cipher image. DNA operation includes DNA addition, DNA subtraction and XOR operation. Huang et al[21]designed a framework for encryption of remote sensing images based on two dimensional logistic map and DNA encoding which is suitable for cryptography but the major drawback of this system is the limited/discontinuous range of chaotic behavior's. Therefore we design a framework that applies Henon map and DNA operations. Therefore we apply Henon map as the pseudorandom number generator. Chaos sequence are used for DNA encoding, DNA mask generation, pixel level and base level arrangement. And hence the encrypted image can be securely transmitted over the channel. The encryption work by Henon map provides more security. However tamper detection still remains to be the main issue.

It is possible to design techniques to find out the tamper detection images. Watermarking techniques has been widely used for finding tamper detection in images. Mohammed et al[22] introduced a dual watermarking scheme for tamper detection but this technique couldn't resist several attacks. Later sawiya et al[23] designed a dual watermarking scheme based on LSB substitution strategy has been proposed and one of the major drawback of this scheme is that it will not be able to recover image tamper if the tampering has occurred globally across the image. Even though the system is easy to implement it is not practical to use it in application where security is an important factor. Madhuri et al[24] proposed a system with 2 Level DWT on RGB components of an image for better security and for tamper detection they make use of a watermarked image as a reference image. The major drawback of this scheme is that it couldn't resist several attacks like cropping, rotate etc. Hutapea et al[25] designed a method of adding confidential information in the remote sensing images using LSB technique. It will insert the confidential information in the rightmost bit in each byte of data, where the rightmost bit has the smallest value. It is easy to implement however lower the security as inserting the information by making smaller changes in the image. Later on Zhang [26] proposed a watermark embedding scheme making use of LSB bits after flipping, to embed the watermark. But the extraction of the entire bit was not guaranteed in this

3. PROPOSED SYSTEM

The proposed framework includes two level of security for the Application. First level is the Encryption scheme by Henon map and DNA coding to prevent information leakage

and to securely transmit an image through any public channel. Second level is the Watermarking scheme in order to find tamper detection of remote sensing images, by adding a unique watermark in to the image. So if the user tries to manipulate the image, then the user can be traced easily by extracting the watermark from the image.

3.1 SYSTEM MODEL

The proposed system is crop insurance system using remote sensing images as shown in Fig.1.It include three modules Farmer, Insurance Company and Image acquisition center.

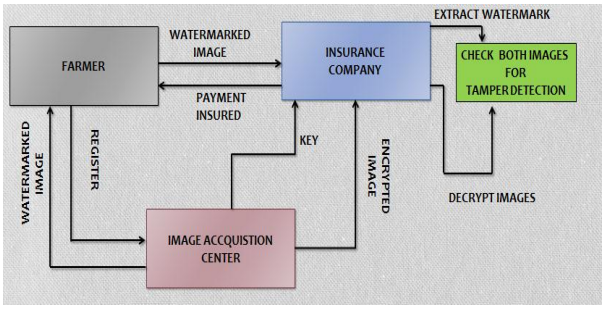

Fig -1: Crop Insurance

3.1.1 IMAGE ACQUISITION CENTER

The image acquisition center act as a central authority. It is trusted for initializing the system and generating secret keys for the participating users. It remotely collects images of crop fields by using various types of aircraft devices. This system encrypts the image and sends to insurance company. In the same image a unique watermark is embedded and a send to the registered farmer.

3.1.2 FARMER

The farmer registers the system and sent a request to the image acquisition center to in order to get the images of the damaged areas of the crop fields. The image acquisition center remotely collects the images of that particular area that is requested by the farmer.so the farmers can make use of this watermarked images of their agricultural fields in order access the insurance claim.

3.1.3 INSURANCE COMPANY

The insurance company would get an encrypted image of the agricultural field that got affected due to hazards from the image acquisition center. Similarly they will get a watermarked image from the farmer and they will check the unique watermark and extract the watermark for tamper detection.

3.2 PRELIMINARY

3.2.1 DNA CODING

Deoxyribonucleic acid (DNA) sequence is an important part in various fields of biological research and numerous applied fields such as diagnostic biotechnology, forensics and biological systematics. DNA encryption is now widely used in international cryptography research[18][20].DNA molecule have several capabilities like low energy consumption, high storage density and have massive parallelism, which is more suitable for image encryption algorithms based on DNA computing. DNA sequencing is the process used to map nucleoside sequence forming a strand of DNA. A single DNA sequence consist of four nucleic acid in the DNA sequence namely A (adenine), T (thymine), C (cytosine),and G (guanine).According to DNA rules A always pair with T,C pair with G, where A and T are complementary. Similarly C and G are complementary [27].This complementary rule resemble to the binary system, as because 0 and 1 are complementary. In the binary system, 00 and 11 are complementary and 01 and 10 are complementary. DNA encoding/decoding rules are in order to fulfil the Watson-crick base pairing rule. In total there are 4! =24 kinds of coding combinations. According to this rules, there are only 8 code combinations which can be used out of 24 code combinations. Table 1 list the DNA encoding/decoding rules . Each pixel in an 8 bit greyscale image can be encoded as 4 base sequences. As an example the pixel value 10010011 can be encoded in to DNA sequence CGAT in Rule 2.The pixel value encoded according to a certain encoding rule will have different value when decode it with other rule. For example CGAT when decode with Rule 4 result in the pixel value 10011100.Hence the encoded image can be decoded with random decoding rules, the plain image can be hidden effectively.

Table -1: DNA Encoding/Decoding Rules

RULES	A	C	G	T
1	00	01	10	11
2	00	10	01	11
3	11	01	10	00
4	11	10	01	00
5	01	00	11	10
6	10	00	11	01
7	01	11	00	10
8	10	11	00	01

Table -2: DNA Addition Rules

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table -3: DNA Subtraction Rules

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

3.2.2 DNA XOR operation

The DNA computing have wide range of applications in biological researchers. As its rapid growth in DNA computing promotes, several algebraic operations like DNA addition, DNA subtraction and XOR operation can be performed. The addition and subtraction operation of the DNA sequence is performed as that like of traditional addition and subtraction in the binary system. According to the DNA decoding schemes there exists 8 kinds of DNA addition rules and DNA subtraction rules. DNA subtraction procedure is the reverse process of DNA addition. Table 2 and Table 3 list DNA addition and subtraction rules. Taking two DNA sequence AGCT and CTGA and adopt the DNA addition operation which would result in the new DNA sequence CATT. Similarly we can also get the sequence AGCT when performing the DNA subtraction in between the sequence CTGA and CATT.

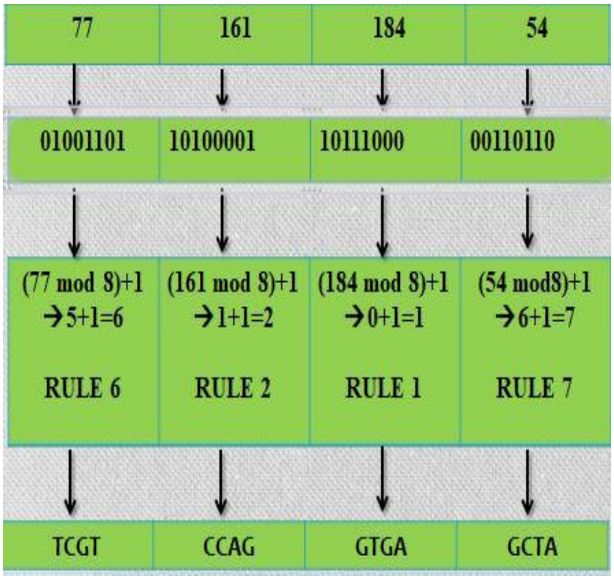

Fig -2: An example of DNA encoding process.

3.2.3 Henon map

The Henon map is also known as Henon pomeau attractor/map is a discrete time dynamical system. The Henon map is a two dimensional chaotic map that takes a point (x_n,y_n) in the plane and map in to a new point in the plane. Henon map is described with the aid of using the subsequent equation:

$$x_{n+1} = y_n + 1 - ax_n^2$$

$$y_{n+1} = bx_n \quad \text{(eq.1)}$$

Henon map represent a 2D chaotic map with non-linearity, basic(ally depends upon two parameters a and b which for a classical Henon map have values a =1.4 and b = 0.3.For this values the system will generate good pseudorandom numbers. Substituting the actual parameters x0 and y0 in eq.(1) and iterating it would produce the required pseudorandom sequence based on Henon map.

3.2.4 WATERMARKING METHOD

Digital watermarking technology is used to verify the authenticity or integrity or to show the identity of users. The watermarking technology is employed for tamper detection in remote sensing images by the farmers in order to get more insurance claim from the insurance company. The color image is initially converted in to a grey scale image. Each pixel in the grey scale image is composed of 8 binary bits. The image is segmented in to non-overlapping blocks and a part of them are randomly chosen to carry watermark bits. Now the pixel in the chosen blocks are randomly divide in to two sets S0 and S1.If the watermark bit is 0,then flip the pixels in S0 and if it is 1,then flip the pixels in S1.Now for the extraction of watermark bits, firstly the blocks having the watermark bits are found according to the secret key. Secondly, the pixels of each block are divided in to two sets S0 and S1 according to Secret key. Flip the pixel by observing the change of fluctuation, it can extract the watermark bit embedded as 1 or 0.The proposed watermarking protocol is designed to find the tamper detection in the images so that the image is owner is prevented from misusing the images.

3.3 CRYPTOSYSTEM

In the framework, first, the farmer will register in to the system and send a request to the image acquisition center in order to claim for crop insurance. The image acquisition center collect the image remotely and watermarking the image using our watermarking scheme and the watermarked image will be given to that particular farmer in order to claim for insurance if they met any natural hazards like flood, earthquake etc. At the same time the same image will be encrypted using the proposed Henon based encryption scheme along with DNA encoding and this could provide better security to the image. The encrypted image will send to the Insurance company. Now the insurance company check for the decrypted image and check for the unique watermark bit sequence in order give the payment.

3.3.1 ENCRYPTION

The permutation–diffusion structure(PDS) is widely used in the field of cryptography. The proposed system works on multiple PDS for DNA random coding and DNA operation, the base level and pixel level rearrangement. In permutation layer, half of the array indexes were applied to permute all the pixels and in diffusion the same indices were associated with the DNA sequence to diffuse the pixel values. Two dimensional Henon map is used as the pseudo random generator in order to yield the coding rule index and DNA mask .The initial parameters of Henon map is used as the security key. The M X N plain image P is encoded in DNA

encoding rules and generate DNA matrix. Similarly the DNA mask matrix is generated from the Henon map. Then execute DNA addition with DNA mask and DNA matrix which forms the list level of encryption. From the resultant matrix, calculate the DNA bases probabilities and substitute again in to the Henon map will result in the generation of pseudo random sequence. The cryptosystem sort the pseudorandom sequence in ascending order to generate an index matrix in order to perform the pixel level and base level rearrangement. After the pixel level and base level rearrangement, it will result in the final cipher image, C.

3.3.1.1 STEPS FOR ENCRYPTION

The encryption procedure is divided into the following steps:

(1) Setting $S = M X N$ and substitute the initial parameters x_0 and y_0 of the Henon map to generate the pseudorandom sequence. Equation (1) is iterated for $S/2+m$ times. Arranging pseudorandom numbers as in Equation (2), we get the chaotic sequence S_p generated by two dimension Henon map.

$$S_P = \{x_{m+1}, x_{m+2}, \ldots, x_{m+S/2}, y_{m+1}, y_{m+2}, \ldots, y_{m+S/2}\} \quad \text{(eq.2)}$$

(2) Convert the sequence S_P into integer vector S_{Pv}.

$$S_{Pv} = |floor(S_P * 255)| \quad \text{(eq.3)}$$

(3) Transform the vector S_{Pv} into a $M X N$ matrix S_{Pm}.

(4) Perform the equation to get the coding rule index

$$Rid = mod(S_{Pm}, 8) + 1 \quad \text{(eq.4)}$$

(5) Generate DNA mask matrix D_{ma} from S_{Pm}.

(6) Plain image P is converted into greyscale and then to binary matrix to generate DNA matrix D_{pm}.

(7) Perform DNA addition between D_{pm} and D_{ma} and get the result Pl according to TABLE 2.

(8) Using count as the function for counting, calculate A,G, C and T.

(10) Calculating their probabilities as follows.

$$pa = \frac{count(A, Pl)}{M \times N}$$
$$pc = \frac{count(C, Pl)}{M \times N}$$
$$pt = \frac{count(T, Pl)}{M \times N}$$
$$pg = \frac{count(G, Pl)}{M \times N} \quad \text{(eq.5)}$$

(11) Calculate the initial parameters as follows.

$$x'_0 = mod(x_0 + \frac{1}{pa} + \frac{1}{pg} + \frac{1}{pc} + \frac{1}{pt}, 1)$$
$$y'_0 = mod(y_0 + \frac{1}{pa} + \frac{1}{pg} + \frac{1}{pc} + \frac{1}{pt}, 1) \quad \text{(eq.6)}$$

(12) Generate self-adaptive chaos sequence S_{PA} by substituting the initial parameters x'_0 and y'_0

$$S_{PA} = \{x'_{m+1}, \ldots, x'_{m+2+S/2}, y'_{m+1}, \ldots, y'_{m+2+S/2}\} \quad \text{(eq.7)}$$

(13) Using a sort function sorts the elements of S_{PA} in ascending order and returns an ordered array *Xpx* and an index vector *Indpx.*

$$[Xpx; Indpx] = sort(S_{PA})$$

(14) Transform the matrix *Pl* into the $M x N$ vector *Kv.*

$$Pr(i) = Kv(Indpx(i)) \quad \text{(eq.8)}$$

Where, i=1,2……..,$M X N$

(15) For the DNA base-level rearrangement,

- Four elements from S_{PA} (i) to S_{PA} $(i + 3)$ are sorted in ascending order
- Returns an ordered array *Xbs(i)* and an index vector *Indbs (i)* of length 4.
- Four bases sequence of *Pr(i)* are rearranged according to the index vector *Indbs(i).*

$$[Xbs(i), Indbs(i)] = sort(Lap(i : i + 3))$$
$$Pb(i)\{j\} = Pr(i)\{Indbs(i)\{j\}\} \quad \text{(eq.9)}$$

(16) Transform the vector into the M x N matrix *Cb.*

(17) Perform the DNA random decoding on the matrix *Cb* according to Equation (4) , the cryptosystem gets the final cipher-image C.

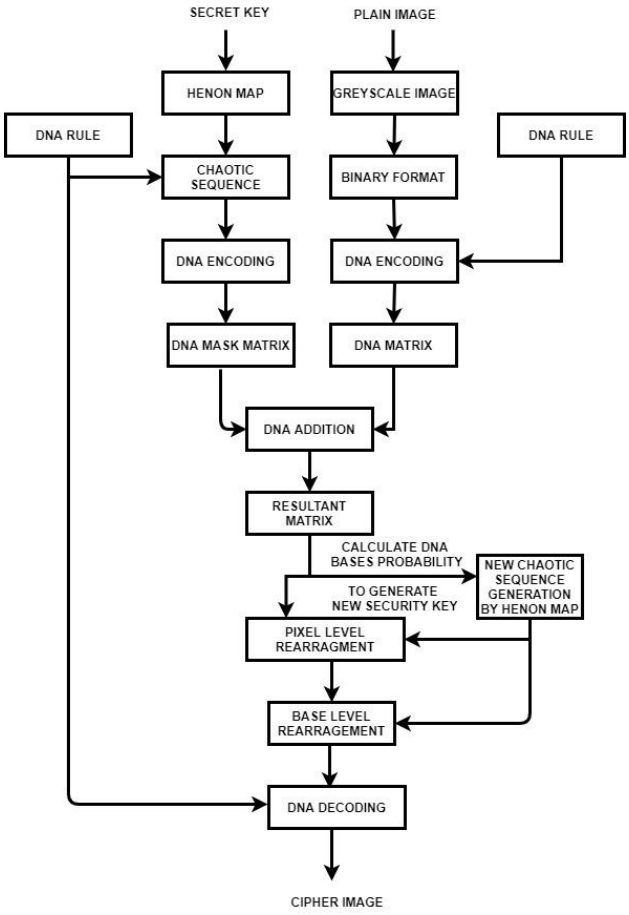

Fig -3: Architecture of Encryption.

3.3.2 DECRYPTION

The decryption is the opposite of encryption. The cipher image will be encoded in DNA encoding rules in order and calculate the DNA bases probabilities of the cipher-image and generate a self-adaptive pseudorandom sequence for reverse pixel level rearrangement and base level rearrangement. The DNA mask matrix is obtained by executing DNA subtraction with the resultant matrix. The DNA matrix is decoded into binary format according to the rules and finally to plain image.

3.3.2.1 STEPS FOR DECRYPTION

The decryption is procedure is the reverse process of encryption

(1) Repeat step(1) in subsection 3.3.1 and generate the chaos matrix S_{pm} and DNA coding rules index *Rid* similar to encryption.

(2)Calculate four DNA bases probabilities of the cipher image C using count function and get *pa,pg ,pc and pt .*

(3) Generate a self-adaptive chaos sequence S_{PA} using equation 6 and 7.

(4)Generate DNA matrix *Cb* from cipher-image C according to *Rid* and Table 1.

(5) Covert matrix *Cb* into the vector *kv*

(6) Executing the reverse DNA base-level rearrangement as follows,

$$[Xbs, Indbs] = sort(Lap(i{:}i+3))$$
$$Pr(i)\{j\} = Pb(i)\{Indbs(j)\} \quad \text{(eq.10)}$$

where, *i*=1,2……..,*M X N and j=1,2,3,4* indicate four DNA bases.

(7) Execute equation (11) for pixel level rearrangement to obtain vector *Kv*

$$Pr(i) = Kv(Indpx(i)) \quad \text{(eq.11)}$$

Where, *i*=1,2……..,*M X N*

(8) Generate DNA mask D_{ma} from the chaos matrix S_{Pm}.

(9) Perform DNA subtraction between Pl and D_{ma} according to Table 3 to obtain DNA matrix $D_{pm.}$

(10) Decoding the DNA matrix $D_{pm.}$ into the M X N matrix E according to Table 1 to obtain plain image.

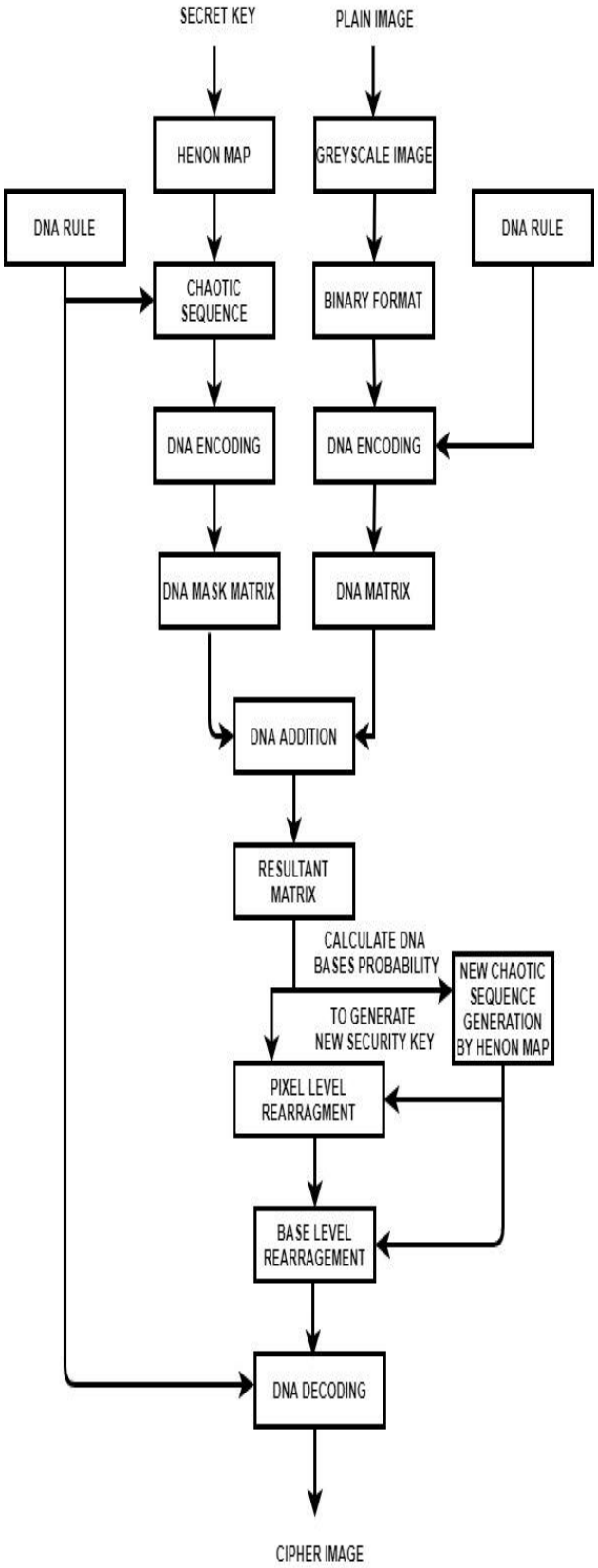

Fig -4: Architecture of Decryption.

3.3.3 WATERMARK EMBEDDING

The pixel in an grayscale image is composed of 8 binary bits. The plain image is segmented into non overlapping blocks and a part of them are randomly chosen to carry watermark bits. Next, the pixels in each of chosen blocks are randomly divided into two sets S_0 and S_1 using a secret key. If the watermark bit is 0, flip all the pixels in S_0.Otherwise, flip all the pixels in S_1. In this way, an watermarked image is generated.

3.3.3.1 STEPS FOR WATERMARK EMBEDDING

(1) Let R be the set of images

(2) Generate secret key k_{emb1},K_{emb2},k_{emb3} and the watermark sequence w ={w_1,w_2,...w_n}

(3) Divide plain text into *s x s* sized non overlapping blocks.

(4) A set of blocks $\{BK\}_{i=1}^{N}$ are chosen by pseudorandom function with the secret key k_{emb1}. Each block will carry one bit of the watermark.

(5) The pixels in block BK_i are divided into two sets S_0 and S_1 according to a pseudorandom function with the secret key k_{emb2}.

(6) If $w_i = 0$, flip the bits of pixels in S_0. Otherwise, flip the pixel bits in S_1.The ratios of flipped bits on 8 bit-planes as $\epsilon = [\epsilon_1, \epsilon_2, ..., \epsilon_8]$.

(7) The flipped positions are determined by k_{emb3}.

(8) Output the watermarked image set R'.

3.3.4 WATERMARK EXTRACTION

The extraction of watermark bits is based on the fluctuation of an original image block is generally lower than that of a flipped one. Initially, the blocks carrying the watermark bits are found according to the secret key. Then the pixels of each block are divided into two sets according to the secret key. Finally, pixels in sets $S0$ and $S1$ are flipped separately. And check the change of fluctuation, we can find the embedded bit is 1 or 0.

3.3.4.1 STEPS FOR WATERMARK EXTRACTION

(1) Let R' be the set of watermarked images.

(2) Let m_t be the image to be extracted then divide it into non overlapping blocks with the size $s \times s$.

(3)Locate the set of blocks $\{BK\}_{i=1}^{N}$ that carries the watermark bits $w = w_1,w_2, ...,w_N$ according to the secret key k_{emb1}.

(4) Divide the pixels in BK_i into two sets S_0 and S_1 according to the secret key k_{emb2}

(5) k_{emb3} to get two blocks BK_i^0 *and* BK_i^1.

(6) Flip the pixels in S_0 and S_1 respectively according to $\{\epsilon i\}_{i=1}^{8}$.

(7) Construct the corresponding block BK_i from the original image with the secret key k_{emb1}.

(8) Calculate $\delta_0 = \sum_{pj \in BKi, pj^0 \in BK_i^0} (p_j^0 - p_j)$ and $\delta_1 = \sum_{pj \in BKi, pj^1 \in BK_i^1} (p_j^1 - p_j)$. If $\delta_0 < \delta_1$, the watermark bit is extracted as '0'. Else, the watermark bit is extracted as '1'

(9) Output the extracted watermark w_t.

The proposed system with encryption along with watermarking provides more security to the system. The application has so many advantages like farmer don't have to collect the images of their damaged agricultural land to claim for the insurance. Instead they have to send a message to the image acquisition center for collecting the exact image of their damaged area in the agricultural land. It would collect the image using latest technologies remotely and will send back to the farmer. Similarly it will be very difficult for crop loss assessors to come check each field.so they will make use of the watermarked images send by the farmer and encrypted images from the image acquisition center. It will extract the unique watermark bit and check for tamper detection and at the same time it will decrypt the image and check the image. The proposed algorithm for encryption and watermarking is highly efficient and can be used in the application for crop insurance. Experimental results show that the proposed algorithm can resist several attacks and at the same time the cipher image generated by using our encryption scheme has uniform distribution, low coefficients and an ideal entropy value. The proposed cryptosystem has an acceptable encryption speed.

4. SECURITY ANALYSIS

There are several analytical methods to evaluate the image encryption and watermarking scheme. We choose three images for evaluating the several aspects of encryption scheme and watermarking on MATLAB R2020a in an Intel Core i3 CPU 2.30GHz AND 4 GB of RAM.

4.1 HISTOGRAM ANALYSIS

An image histogram reveals the tonal representation of image. It can plot the number of pixels corresponding to tonal value. It provide the information about the pixel value distribution y counting the number of each grey scale values. An encryption scheme will have a uniform distribution in the cipher mage so that it will be very difficult for the attacker to gain information from the cipher image. Figure 10 and Figure 9 shows the plain images will be having the pixel value concentration on some pixels while that the cipher images will be having uniform distribution.

Variance of a histogram defines the statistics about the distribution of uniformity of pixels. If the value of variance is lower then higher will be the uniformity of image. The variance of a histogram is defined by the following equation

$$var(P) = \frac{1}{256^2} \sum_{i=1}^{256} \sum_{i=1}^{256} (P_i - P_j)^2$$

Where P is the vector of the histogram values and $P = \{p_1, p_2, ..., p_{256}\}$. p_i and p_j are the numbers of pixels which values are equal to i and j respectively.

Fig -5: Plain image 1

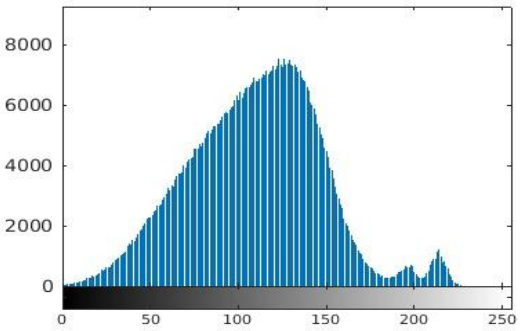

Fig -6: Histogram of Plain image 1

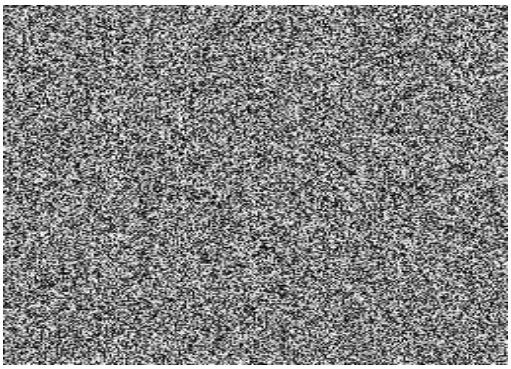

Fig -7: Cipher image 1

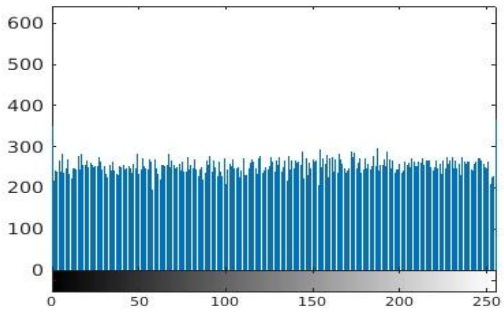

Fig -8: Histogram of cipher image 1

Fig -9: Plain image 2

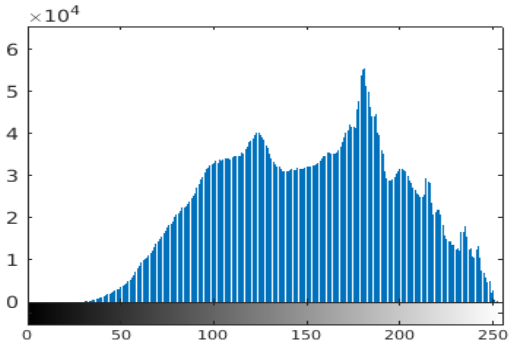

Fig -10: Histogram of plain image 2

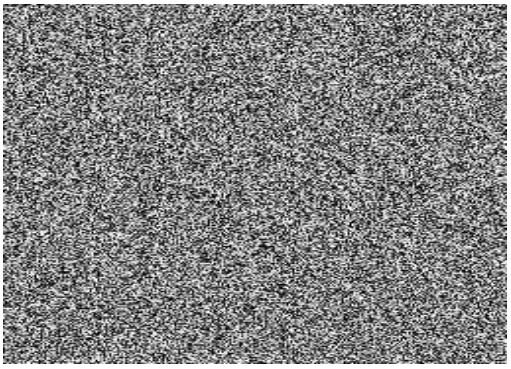

Fig -11: Cipher image of plain image 2

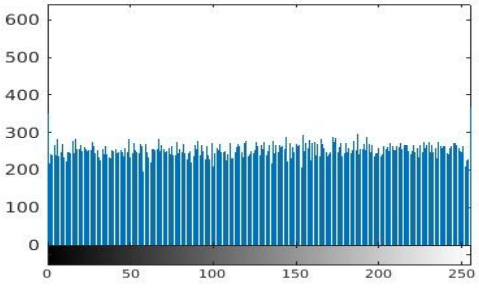

Fig -12: Histogram of cipher image 2

Fig -13: Plain image 3

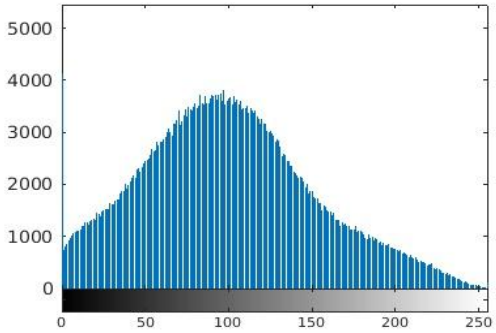

Fig -14: Histogram of plain image 3

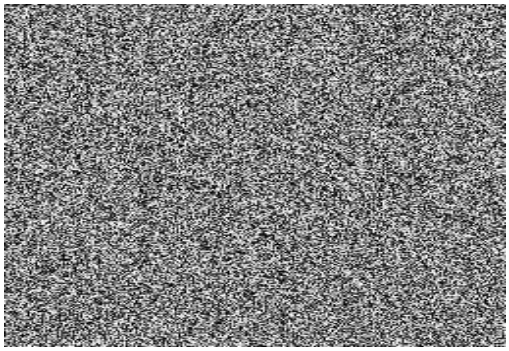

Fig -15: Cipher image of plain image 3

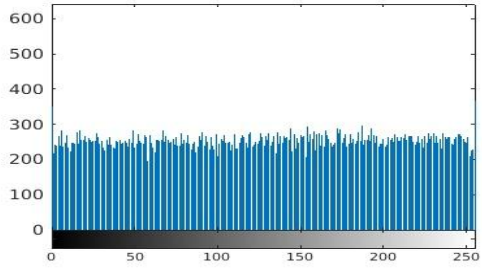

Fig -16: Histogram of cipher image 3

Variances of cipher-images are smaller than plain-images. Therefore, the cryptosystem can resist statistical analysis.

Table -4: Variance of histogram

IMAGES	PLAIN IMAGE 1	PLAIN IMAGE 2	PLAIN IMAGE 3
PLAIN IMAGE	50324	1895531	104524
CIPHER IMAGE	278	1022	227

4.2 CORRELATION ANALYSIS

The adjacent pixel in remote sensing images is very close to each other so that they are having high degree of correlation. But the cryptosystem to be more secured the correlation between the two adjacent pixels should be very low. Correlation coefficient [28][29] is used to measure the relationship between two variables. It may be described via way of means of the subsequent equation

$$E = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{S}(x_i - E(x))^2$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

Here x and y denote the adjacent pixels and S is the total number of pixels selected from an image. E(x) represent mathematical expectations and D(x) is the of variance of x. Cov (x, y) is represent the covariance between x and y. rxy represents correlation coefficient of an image. Figure 17 and 18 plot correlation distributions along horizontal, vertical and diagonal directions for plain image1. Correlation distributions of plain-images are concentrated while of cipher-images are fairly uniform. So the proposed cryptosystem can effectively reduce the correlation between two adjacent pixels along three different directions. We calculate correlation coefficients for three plain images and their cipher-images along horizontal, vertical and diagonal direction. Results of correlation coefficients are indexed in Table 5 and 6. For a good cryptosystem the correlation coefficients of plain-images are closed to 1 while those of cipher-images are closed to 0. Therefore, the attacker cannot get valuable correlation information to break up the cryptosystem by correlation analysis.

Table -5: Correlation coefficients of adjacent pixels in plain image 1

SCAN DIRECTION	PLAIN IMAGE 1	PLAIN IMAGE 2	PLAIN IMAGE 3
HORIZONTAL	0.9723	0.9703	0.7938
VERTICAL	0.9279	0.9742	0.8612
DIAGONAL	0.9081	0.957	0.8970

Table -6: Correlation coefficients of adjacent pixels in cipher image 1

SCAN DIRECTION	CIPHER IMAGE 1	CIPHER IMAGE 2	CIPHER IMAGE 3
HORIZONTAL	-0.0001	-0.0022	-0.0033
VERTICAL	0.0022	-0.0035	-0.0006
DIAGONAL	-0.0039	-0.0092	-0.0049

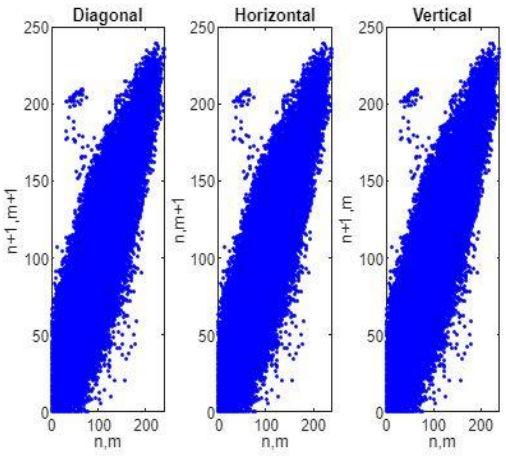

Fig -17: Correlation of two adjacent pixels in plain image

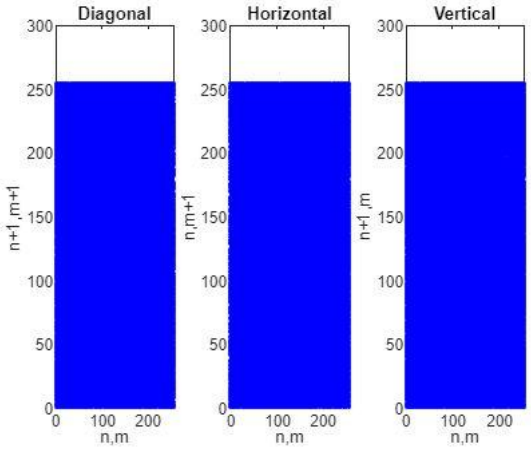

Fig -18: Correlation of two adjacent pixels in cipher image

4.3 INFORMATION ENTROPY

Information entropy is an important feature of randomness. The entropy describes about the average information content. Information entropy [30][31] measure the intensity of a symmetric cryptosystem. The information entropy is defined by the mathematical equation,

$$H(y) = -\sum_{i=0}^{2^n-1} p(y_i) log_2 p(y_i)$$

Here in this equation, p(yi) is the probability of the symbol yi. The perfect value of entropy is same to eight for the cipher-image Larger information entropy indicates less information content in the image. Table 7 reports information entropy of plain-images and their cipher-images. Results show that the cryptosystem less image information.

Table -7: Information Entropy

IMAGES	PLAIN IMAGE 1	PLAIN IMAGE 2	PLAIN IMAGE 3
PLAIN IMAGE	7.2404	7.5284	7.6690
CIPHER IMAGE	7.9958	7.9961	7.9952

4.4 DIFFERENTIAL ATTACK

The fundamental requirement for all image encryption schemes is that the encrypted image needs to be exclusive from its unique version. This difference can be measured by means of two parameters: namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). NPCR is the change in rate of the encrypted

image pixels when the image changes one pixel in the process during encryption. NPCR will calculate the proportion of various pixel numbers among cipher photos and in addition the UACI will calculate the common depth of distinction among cipher images. The larger the value for NPCR is, the stronger the resistance is of the algorithm to plaintext attack. UACI is the change rate of the of the original image and the encrypted image. The larger value for UACI is, the stronger the resistance is of the algorithm to differential attacks [33].NPCR and UACI are defined by the following equation,

$$D(i,j) = \begin{cases} 0, & C(i,j) = C(i,j)' \\ 1, & C(i,j) \neq C(i,j)' \end{cases}$$

$$NPCR = \frac{\sum i,jD(i,j)}{M\ X\ N}\ X\ 100\%$$

$$UAC1 = \frac{1}{M\ X\ N}\left[\sum_{i,j}\frac{|C(i,\ j) - C(i,\ j)'|}{255}\right] X\ 100\%$$

where M X N is the size of cipher-images C and C'. Table 8 reviews common effects of NPCR and UACI for 1 bit pixel alternate withinside the random pixel of the plain-image, which can be closed to best value. Results show that the proposed algorithm can resist differential attack.

Table -8: Average NPCR and UACI for differential analysis

IMAGES	NPCR (%)	UACI (%)
PLAIN IMAGE 1	99.29	33.50
PLAIN IMAGE 2	99.52	33.45
PLAIN IMAGE 3	99.77	33.33

4.5 ENCRYPTION EFFICIENCY

Encryption efficiency [32] represents the running performance of the encryption scheme. Multiplication of floating point numbers is the time consuming part in chaos based encryption schemes. The cryptosystem require Θ(2 X T X N) iterations of multiplying floating point numbers as Henon map is executed twice. Due to large time consuming of DNA coding and DNA operation, the cryptosystem based on DNA coding is not usually of high efficiency and the corresponding time complexity is Θ(T X N) The time complexity for pixel level arrangement is Θ(T X N) and base level arrangement is Θ(4 X T X N) .We stimulate the encryption process for 100 times and computed the encryption speed of 0.713054 Mbits/s, which is an acceptable running speed for a cryptosystem. The propose system has high parallel operation in DNA coding and DNA operation.

4.6 TIME CONSUMPTION FOR WATERMARKING

The watermarking scheme embeds watermark bits by flipping image pixels according to each bit flipping proportion as ϵ = [ϵ1ϵ2.....ϵ8]. The number of the flipped bits equals $\sum_{i=1}^{8} \epsilon i$ x N X S/2 . The time complexity of flipping is O(N X S).The times consumed by the flipping of bits and the whole embedding process are listed in Table 7 and 8. The results are evaluated by embedding process of 1000 images The bit flipping ratios are set to values [0, 0, 0,0.1, 0.2,0.4, 0.8, 0.9]. Table 9 and 10 show that the time consumed by the flipping is only a small portion of the time consumed by the whole embedding process.

Table -9: Time consumed by bit flipping (*ms*)

Number of watermark bits	Size of block *S*		
	16	24	32
16	0.122	0.258	0.475
24	0.244	0.543	0.951
32	0.492	1.092	1.823

Table-10: Time consumed by the whole watermark embedding process (ms)

Number of watermark bits	Size of block *S*		
	16	24	32
16	4.933	5.121	5.154
24	5.091	5.257	5.608
32	5.471	5.836	6.657

4.7 PEAK SIGNAL TO NOISE RATIO (PSNR)

It represents the amount of distortion due to embedding process. For 8 bit data typical values for the PSNR are between 30 and 50dB.

Fig -19: Original Image

Fig -20: Watermarked Image with PSNR =37.752

5. DISCUSSION

The paper proposes a secure application of crop insurance using DNA cryptography, Henon map and a watermarking protocol by making use of remote sensing images as it contain the correct and relevant information. Here we analyzed the security of the application by different methods like histogram analysis, correlation analysis, information entropy, differential attack, running performance and peak signal to noise ratio. The experimental results show that the proposed application of crop insurance could resist various attacks. In order to withstand chosen-plaintext and differential attack, we designed an encryption scheme that build a close connection between plain image and cipher image by making use of DNA cryptography and two dimensional Henon map. Table 11 shows the comparison of average NPCR and UACI for differential attack with the algorithms [14],[19] and [33]. The comparison shows that the proposed method could resist differential attack.

Algorithm	NPCR	UACI
Ideally	0.996094	0.33435
Proposed	0.998145	0.33554
[14]	0.997570	0.39125
[19]	0. 996124	0. 33401
[33]	0.993611	0.33144

Chart 1 shows the comparison of average information entropy with proposed algorithm based on DNA cryptography and two dimensional Henon map. The comparison chart shows that our proposed encryption scheme has higher security than other algorithms. Chart 2 shows the comparison of PSNR value with other methods. The comparison chart shows the proposed method has better PSNR value than other watermarking methods.

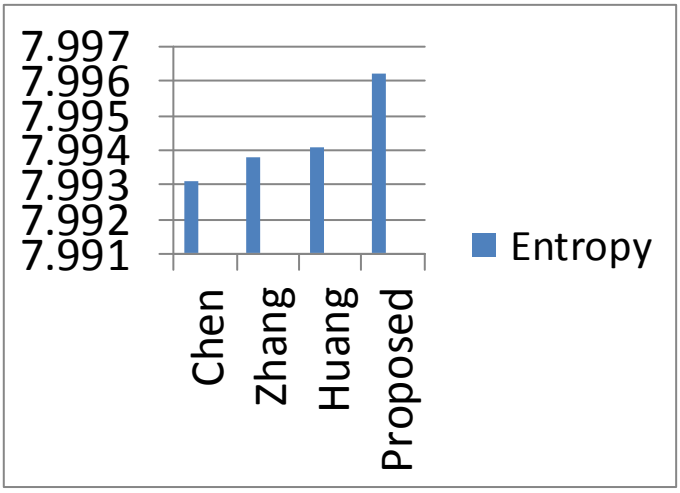

Chart -1: Comparison of Average Information Entropy.

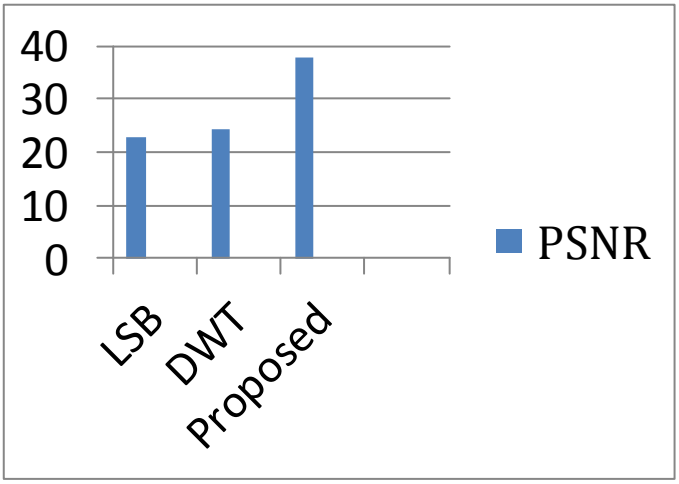

Chart -2: Comparison of PSNR value.

6. CONCLUSION

A secured application for crop insurance using two dimensional Henon map and watermarking protocol. By using this application the farmer can easily request for insurance claims. The application incorporates watermarking scheme thus resist tampering. Simulations shows that the cipher image generated have fairly uniform distribution, high information entropy and high PSNR value. The cryptosystem have an encryption speed of 0.713054 Mbits/s. The experimental results show that it can resist several attacks. So the proposed. System can provide high security for remote sensing images.

REFERENCES

[1] U., R. B., Desai, V. V., Ajawan, P. S., & Jha, S. K. (2018). Remote Sensing Technology and Applications in Agriculture. 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS). doi:10.1109/ctems.2018.8769124

[2] Kalluri, S., Plante, R., Mohamed, M., Bergman, R., & Carr, K. (n.d.). Remote sensing applications for

operational decision making at local scales: current status and future opportunities for agriculture and disaster management applications. IGARSS 2001. Scanning the Present and Resolving the Future. Proceedings. IEEE 2001 International Geoscience and Remote Sensing

[3] Youcun, L., Bo, S., Baisheng, Y., & Tianding, H. (2010). The application of remote sensing technology in the glacier change monitoring of Yulong Mountain. The 2nd International Conference on Information Science and Engineering.

[4] Kingra, Pavneet, Majumder, Debjyoti, Singh, Som Pal, "Application of Remote Sensing and GIS in Agriculture and Natural Resource Management Under Changing Climatic Conditions", Agricultural Research Journal, 53, pp. 295-302, October, 2016..

[5] V.C.Patil, K.A.A1-Gaadi, D.P.Biradar, M.Rangaswamy, "Internet of Things (IoT) and Cloud Computing for Agriculture: An Overview", Proc. of AIPA, India, 2012.A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[6] Zhao, Q., & Liu, Y. (2012). Remote Sensing Monitoring System for Agriculture Condition. 2012 Fourth International Conference on Computational and Information Sciences.

[7] Teke, M., Deveci, H. S., Haliloglu, O., Gurbuz, S. Z., & Sakarya, U. (2013). A short survey of hyperspectral remote sensing applications in agriculture. 2013 6th International Conference on Recent Advances in Space Technologies (RAST)..

[8] Salima, Y., Peira, J. F. M., horra, G. rincon de la, & Ablanque, P. V. M. (2019). Remote Sensing Data: Useful Way for the Precision Agriculture. 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS).

[9] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan,``Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller,'' *Micro-process. Microsyst.*, vol. 56, pp. 1_12, Feb. 2018D.

[10] L. Teng, X. Wang, and J. Meng, ``A chaotic color image encryption using integrated bit-level permutation,'' Multimedia Tools Appl., vol. 77, no. 3,pp. 68836896, 2018.

[11] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, ``An image encryption algorithm based on chaotic system and compressive sensing,'' Signal Process., vol. 148, pp. 124144, Jul. 2018.

[12] A. Ullah, S. S. Jamal, and T. Shah, ``A novel scheme for image encryption using substitution box and chaotic system,'' Nonlinear Dyn., vol. 91, no. 1,pp. 359370, 2018.

[13] X. Chai, Y. Chen, and L. Broyde, ``A novel chaos-based image encryption algorithm using dna sequence operations,'' Opt. Lasers Eng., vol. 88, pp. 197213, Jan. 2017.

[14] Mondal, B., & Mandal, T. (2017). A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University - Computer and Information Sciences, 29(4), 499–504. doi:10.1016/j.jksuci.2016.02.003

[15] R. Enayatifar, F. G. Guimar aes, and P. Siarry, ``Index-based permutationdiffusion in multiple-image encryption using DNA sequence,'' Opt. Lasers Eng., vol. 115, no. 3, pp. 131140, 2019.

[16] M. Li, Y. Guo, J. Huang, and Y. Li, ``Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure,'' Signal Process., Image Commun., vol. 62, no. 3, pp. 164172, 2018.

[17] P.Gunavathy et al, segmentation and encryption of satellite images using stream cipher algorithm International Journal of Computer Science and Mobile Computing, Vol.5 Issue.5, May- 2016, pg. 743-750.

[18] A. Gehani, T. LaBean, and J. Reif, ``DNA-based cryptography,'' Aspects Mol. Comput., vol. 54, no. 3, pp. 233249, 2004

[19] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, ``Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption,'' Signal Process., vol. 142, pp. 340353,Jan. 2018.

[20] J. Wu, X. Liao, and B. Yang, ``Image encryption using 2D HénonSinemap and DNA approach,'' Signal Process., vol. 153, no. 3, pp. 1123,Dec. 2018.

[21] Liu, H., Zhao, B., & Huang, L. (2019). A remote-sensing image encryption scheme using DNA bases probability and two dimensional logistic map. IEEE Access, 1–1. doi:10.1109/access.2019.2917498

[22] Saiyyad, M. A. M., & Patil, N. N. (2014). Authentication and tamper detection in images using dual watermarking approach. Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization.

[23] Kiatpapan, S., & Kondo, T. (2015). An image tamper detection and recovery method based on self-embedding dual watermarking. 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecomm - unications and Information Technology (ECTI-CON).

[24] Rajawat, M., & Tomar, D. S. (2015). A Secure Watermarking and Tampering Detection Technique on RGB Image Using 2 Level DWT. 2015 Fifth International Conference on Communication Systems andNetworkTechnologies.doi:10.1109/csnt.2015.245

[25] Destri Yanti Hutapea1, Octaviani Hutapea, waterm-arking method of remote sensing data using

steganography technique based on least significant bit hiding International Journal of Remote Sensing and Earth Sciences Vol. 15 No. 1 June 2018: 63 – 70

[26] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[27] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," Journal of Systems and Software, vol.85, no. 2, pp. 290–299, 2012.

[28] U. Hayat and N. A. Azam, ``A novel image encryption scheme based on an elliptic curve,'' Signal Process., vol. 155, no. 3, pp. 391402, 2019.

[29] L. Huang, S. Cai, M. Xiao, and X. Xiong, ``A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion,'' Entropy, vol. 20, no. 7, pp. 535554, 2018.

[30] M. L. Sahari and I. Boukemara, ``A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption,'' Nonlinear Dyn., vol. 94, no. 1, pp. 723744, Oct. 2018.

[31] Y. Zhang, ``The unied image encryption algorithm based on chaos and cubic S-box,'' Inf. Sci., vol. 450, no. 3, pp. 361377, 2018

[32] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, ``A color image cryptosystem based on dynamic DNA encryption and chaos,'' Signal Process., vol. 155, pp. 4462, Feb. 2019.

[33] X. Zhang and X. Wang, ``Remote-sensing image encryption algorithm using the advanced encryption standard,'' Appl. Sci., vol. 8, no. 3, pp. 15401552, 2018.

[34] Seema Malshe (Gondhalekar), Hitesh Gupta, Saurabh Mandloi, Survey of Digital Image Watermarking Techniques to Achieve Robustness, International Journal of Computer Applications(0975-8887), Volume 45, No.13, May 2012.