ENCRYPTION ALGORITHM BASED ON CHAOTIC SEQUENCE AND PLAIN TEXT

BY:
DIVYA NAGAR & SHRESHTHA GARG

WHAT IS ENCRYPTION?

Encryption: As the name says the activity of converting data or information into code.

It is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Unencrypted data is called plain text ;

encrypted data is referred to as cipher text.

WHY CHAOTIC SEQUENCE?

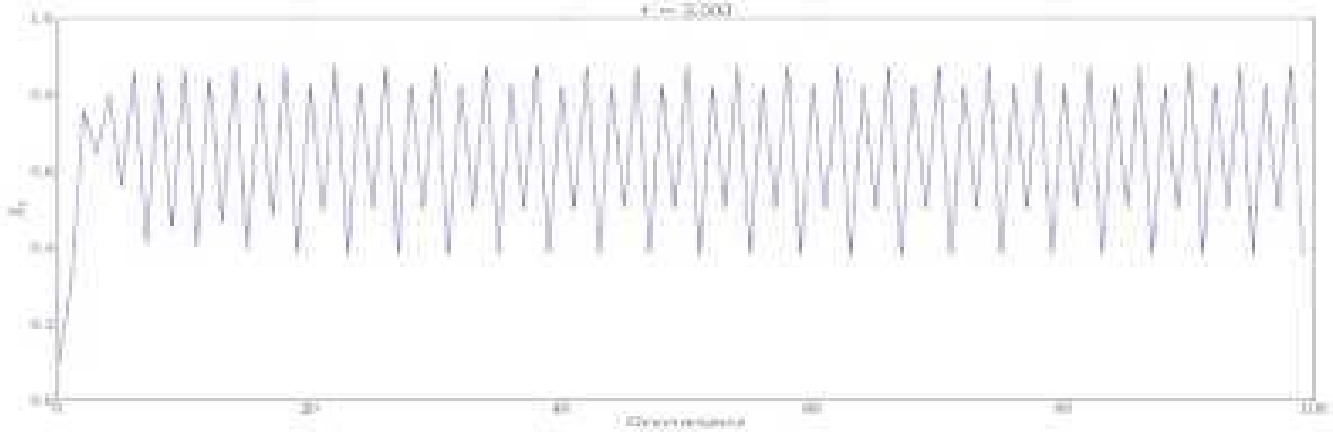
Chaotic behaviour is complex, but nevertheless can be observed in fairly simple dynamical systems. Chaotic signals are irregular, aperiodic, uncorrelated and impossible to predict over longer times.

And when predictions fail your decryption fails as well.

LOGISTIC MAP BEHAVIORS

$$X_{(i+1)}=r*X_{(i)}*(1-X_{(i)})$$

Most values beyond 3.56995 exhibit chaotic behaviour.



ABSTRACT

In this algorithm a key is generated which is based on chaotic sequence and plain text. The key does not allow to decrypt the ciphertext even on having initial values since it is based on chaotic sequence and plain text. Key is used to encrypt the plaintext and again to decrypt the ciphertext.

KEY GENERATION & ENCRYPTION

1. Binary Chaotic Sequence(S) is generated using logistic map at parameter value r=4.
2. converted the sequence into matrices form of size equivalent to image.
3. Plaintext(P) is operated with the binary chaotic sequence and the Key(K) is generated.

$$K(i,j) = P_{(i,j)} \odot S_{(i,j)} \quad \{\text{where } i=1,2,3\ldots..\}$$

4. The key is operated with the Plaintext and the Ciphertext(C) is generated and key is saved.

$$C_{(i,j)} = K_{(i,j)} \oplus P_{(i,j)} \quad \{\text{where } i,j=1,2,3\ldots..\}$$

A	B	A⊕B
1	1	0
0	1	1
1	0	1
0	0	0

A	B	A⊙B
1	1	1
0	1	0
1	0	0
0	0	0

DECRYPTION

Using the saved key and ciphertext decryption is being done and plaintext is successfully obtained.

$$P_{(i,j)} = K_{(i,j)} \oplus C_{(i,j)} \quad \{\text{where } i,j=1,2,3\ldots.\}$$

EXAMPLE

ENCRYPTION

P = 101111110001

S = 111111000001

K = S⊙P = 101111000001

C = K⊕P = 000000110000

DECRYPTION

K = 101111000001

C = 000000110000

P = K⊕C = 101111110001

ENCRYPTION MATLAB CODE

```
img=imread('lena1.jpg');
BW = im2bw(img,0.4);
r= 3;
 x(1) = .43;
N    = 25599;
for i = 1:N
        x(i+1) = r*x(i)*(1 - x(i));
end
```

```
for i=0:N
        if x(i+1)>.65
                x(i+1)=1;
        else
                x(i+1)=0;
        end
end
[mat,padded] = vec2mat(x,160);  % Created A matrix of 160x160 using chaotic sequence.
lf=find(mat);
for i=1:160
        for j=1:160
                k(i,j)=BW(i,j)*mat(1,j);  % Key generation
                c(i,j)=k(i,j)+BW(i,j);      % Got the ciphertext
                if c(i,j)==2
                        c(i,j)=0;
                 end
        end
end
imshow(c);   //
save('key.mat','k');   % save the key
```

DECRYPTION MATLAB CODE

```
for i=1:160
        for j=1:160
                d(i,j)=k(i,j)+c(i,j);  %Using the previous key to decrypt
                if d(i,j)==2
                        d(i,j)=0;
                  end
        end
end
imshow(d);
```

MATLAB TESTS

1. Data is taken from the original image.
2. Using initial parameters a cipher image (img-2) is generated and key is stored.
3. Using same key the cipher is decrypted and original image (img-3) is obtained.
4. Performed small changes in initial parameters and generated another key to decipher which gave us image (img-4).

ORIGINAL

IMG-1

IMG-2

IMG-3

IMG-4

CONCLUSION

In this algorithm plain text is being used to generate the key which makes it more difficult to decrypt the ciphertext.

Use of chaotic sequence makes the ciphertext more uncorrelated to plaintext and fails all kind of predictions.

This algorithm fails plaintext attack completely because the entire plaintext is being used for key generation.

BIBLIOGRAPHY

1. Nonlinear dynamics and chaos Steven H. Strogatz.
2. Jun Peng, Du Zhang,Xiaofeng Liao, A Novel Algorithm for Block
3. Encryption of Digital Image Based on Chaos [2005] A Proposed Encryption Scheme based on Henon Chaotic System for Image Security [International Journal of Computer Applications (0975 – 8887) Volume 61– No.5, January 2013]

4. Xing-Yuan Wang, Sheng-Xian Gu, New chaotic encryption algorithm base on chaotic sequence and plain text. [Published in IET Information Security,doi: 10.1049/iet-ifs.2012.0279, 2013]