ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

# A Modified Approach for Symmetric Key Cryptography Using Circles

Deepti Rana [1], Shivani Saluja [2]

Assistant Professor, Department of Computer Science, ABES College of Engineering, Gaziabad, U.P., India[1]

Assistant Professor, Department of Computer Science, ABES College of Engineering, Gaziabad, U.P., India[2]

**ABSTRACT**: Cryptography is the science or art of transforming an intelligible message(plaintext) into one that is unintelligible(cipher text) and then transforming the message back to its original form. . Symmetric key Cryptography is a cryptographic approach where the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message Geometry based cryptography is a new and emerging approach in the field of cryptography. It uses geometric shapes such as circles, ellipses etc and perform geometric transformations on these figures to produce cipher text. The presented work focuses on the Symmetric key Cryptography technique, using the concepts of Cartesian coordinate geometry and circle generation. Chakra algorithm, for symmetric key cryptography, is used as the basis for this work with some modifications in it for better results. Chakra is a Sanskrit term which means a circle or a disc. It plays a key role in encryption of data. Data is grouped into circles and each circle holds a portion of data. An improved geometric cryptographic algorithm is developed, that considers data into a 2- dimensional data grid, generate circles on the grid and apply some geometric transformations over data. This encryption technique adapts hybrid geometric transformations,(i.e., translation followed by scaling ) of the circumference points of every circle by some scaling factors(S,Sy) and translation factors(Tx,Ty). The proposed algorithm is an improvement in the basic Chakra algorithm in terms of accuracy.

**KEYWORDS**: Geometric Cryptography, Geometric transformations, Symmetric key cryptography, Data grid, inverse transformations, scaling, translation.

## I. INTRODUCTION

CRYPTO means “SECRET” ,GRAPHY means “WRITING”. Cryptography is the science or art of transforming an intelligible message(plaintext) into one that is unintelligible(cipher text) and then transforming the message back to its original form. It can be said that cryptography is the practice and study of techniques for secure communication in the presence of third parties.

Symmetric key Cryptography is a cryptographic approach in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES).Others are Triple DES(TDES) and Advanced Encryption Standard(AES).

Geometry based cryptography is a new and emerging approach in the field of cryptography. Geometric algorithms are always difficult to decrypt as compared to other traditional algorithms .It uses geometric shapes such as circles, ellipses, etc and perform geometric transformations on these figures to produce cipher text.

Chakra algorithm, for symmetric key cryptography, is used as the basis for this work with some modifications in it for better results. “Chakra” means a circle or a disc. It plays a key role in encryption of data. Data is grouped into circles and each circle holds a portion of data. An improved geometric cryptographic algorithm is developed, that

DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

considers data into a 2- dimensional data grid, generate circles on the grid and apply some geometric transformations over data. This encryption technique adapts hybrid geometric transformations,(i.e., translation followed by scaling ) of the circumference points of every circle by some scaling factors($S_xS_y$) and translation factors(Tx,Ty). The proposed algorithm is an improvement in the basic Chakra algorithm in terms of accuracy.

## II. RELATED WORK

### BASIC CHAKRA ALGORITHM FOR SYMMETRIC KEY CRYPTOGRAPHY

The basic "Chakra algorithm" is a symmetric key encryption technique. It is a 2d geometry based encryption technique which uses the concepts of Cartesian coordinate geometry and circle generation. This algorithm considers data into a 2- dimensional data grid which is similar to the Cartesian plain , generate circles on data grid and also use the process of translation and rotation ,on circumference points of every circle. Unlike other current algorithms, in chakra algorithm, we will not directly change the data, instead the location of data.

Data types used in the algorithm are:

1. X-Length (XL): Length of the x-axis in the grid.
2.Y-Length (YL): Length of the y-axis in the grid.
3. r: Radius of the circle.
4. Pattern (P n): The fashion in which the circles in grid are rotated (1-Horizontal, 2-Horizontal snake pattern,3-vertical, 4-vertical snake pattern)
5. Grid: array collection of points (XL*YL).
6 .P: Length of bit stream of plain text (bit 0 or 1).
7. Point(x, y, data bit): user defined data class contains x-Coordinate value, y-Y Coordinate value and Data Bit (binary 0 or 1).
8. Circle: User defined data class contains Circle Centre (xc, yc), X Coordinate and Y Coordinate.

Major steps in the basic Chakra Algorithm:

Step 1: Collect data from the sender:

XL: X-Length
YL:Y-Length
r: radius
Pn: Pattern
P-Plaintext (stream of bits)

Step 2: Create Cartesian Grid plain (XL*YL)

In creation of grid verify the following conditions:

If P = (XL*YL) then create grid with (XL*YL) points
Else
If P < (XL*YL) then fill the grid points with noise value.
Else
If P > (XL*YL) then re-enter the value of XL and YL.

Step 3: Generate circles on the grid using "Bresenham's circle drawing algorithm".

**Bresenham's circle generation algorithm:**

In computer graphics, the midpoint circle algorithm is an algorithm used to determine the points needed for drawing a circle. The algorithm is a variant of Bresenham's line algorithm, and is thus sometimes known as Bresenham's circle algorithm.The algorithm starts with the circle equation x^2 + y^2 = r^2. For simplicity, assume the centre of the circle is at (0,0).

i. Consider only the first octant and draw a curve which starts at point (r,0) and proceeds counter clockwise, reaching the angle of 45.The "fast" direction here (the basis vector with the greater increase in value) is the y direction. The algorithm always takes a step in the positive y direction (upwards), and occasionally takes a step in the "slow" direction (the negative x direction).
ii. From the circle equation we obtain the transformed equation x^2 + y^2 - r^2 = 0, where r^2 is computed only a single time during initialization.

DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

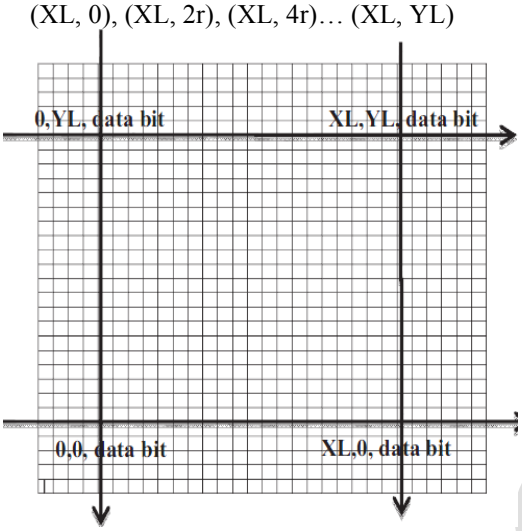
International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

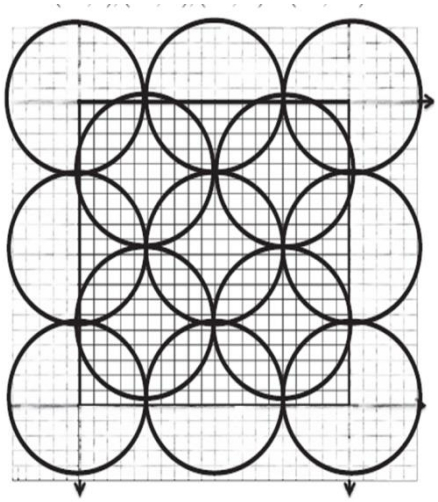
**Vol. 3, Issue 12, December 2014**

Let the points on the circle be a sequence of coordinates of the vector to the point (in the usual basis). Generate circles using Bresenham's circle generation algorithm(Fig:1(b)) with centers as shown below:

(0, 0),(0, 2r),(0, 4r)….(0, YL)
(r, r),(r, 3r), (r,5r)….(r,YL-r)
(2r, 0), (2r, 2r), (2r, 4r)… (2r, YL)
(3r, r),(3r, 3r), (3r,5r)… (3r, YL-r)
(XL, 0), (XL, 2r), (XL, 4r)… (XL, YL)




(a)



(b)

Fig 1:(a) Generation of the 2D data grid

Fig 1: (b) Generation of circles over the 2D grid

Step 4: Add 1 bit of data at every integral Cartesian point that lies on the circle.
Step 5: Perform translation and rotation of these circles so that bit position is changed..Follow the pattern which is given by the user.

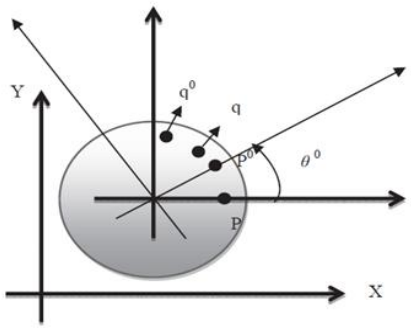



Fig 2: Rotation transformation

The transformation equation for rotating a point at position (x,y)as shown in Fig 2 through an angle θ is:

$x' = x\cos\theta - y\sin\theta$
$y' = x\sin\theta - y\cos\theta$

The rotation equation in the matrix form:

$P' = R.P$

Where R is a rotation matrix

$$R = \begin{vmatrix} \cos\theta & -\sin\theta \\ \sin\theta & -\cos\theta \end{vmatrix}$$

DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

Step 6: Cipher text is obtained.

**Key Composition in the basic Chakra algorithm :**

The key used in this algorithm will consist of mainly following components:

i. Radius of the circle
ii. Length of the Cartesian plain
iii. Breadth of the Cartesian plain
iv. Array of angles each circle is rotated
v. Pattern of rotation (optional)
vi. Starting point of the first circle (optional)
vii. Variable array of radius (Optional)
viii. A circle of random bits(optional)

**Decryption in the basic Chakra algorithm:**

When all the bits collected from the key, the receiver will know what is the pattern size of the grid, pattern selected for encryption, anti-rotate circle by how much angle i.e. rotate by $-\theta$ for every $\theta$ .

Since all are invertible functions, at the end plain text is achieved.

**Drawbacks of the basic approach:**

This basic chakra algorithm encryption technique adapts rotation of circumference points with some angle for all circles. The drawbacks in chakra algorithm are the sine and cosine functions used during rotation of a circle which mostly give irrational numbers making it difficult to store the original value. A circle is rotated by 45° then the point (1,1) becomes (0,1.414..) the irrational numbers causing the problem. The rotational angle (90°,180° etc) are only possibilities where both sine and cosine functions are rational numbers."So, this is the main drawback of this algorithm.

## III. PROPOSED APPROACH

The proposed approach designs an improved geometric cryptographic algorithm using hybrid geometric transformations (i.e translation and scaling). This work is basically an improvement in the basic Chakra algorithm in terms of accuracy.

Modifications in the basic approach: Instead of using the rotation as transformation which uses sine and cosine functions, some other combined transformations are used, i.e. translation followed by scaling for each circle, to increase the accuracy in the results.

Scaling transformations stretch or shrink a given object and, as a result, change lengths and angles. The meaning of scaling is making the new scale of a coordinate direction p times larger. In other words, the x coordinate is "enlarged" p times. This requirement satisfies x' = p x and therefore x = x'/p. Scaling can be applied to all axes, each with a different scaling factor.

The Key Composition in the proposed approach:

The new key in the proposed approach is composed of the following components:

i. Radius of the circles
ii. Centre of the circles
iii. Length of the Cartesian plain
iv. Breadth of the Cartesian plain
v. Scaling factors(Sx,Sy)
vi. Translation factors(X-shift,Y-shift)
vii. Starting point(reference point)
viii. Pattern of hybrid transformation.

DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

## IV. MAJOR STEPS IN THE PROPOSED ALGORITHM

The major steps in the current approach can be summarized as follows(Fig 3):

1. Accepting a message file.
2. Converting it to binary.
3. Creating a 2-dimensional Cartesian grid plain and generating circles on it(using Bresenham's Circle generation algorithm).
4. Adding 1 bit of data at every integral Cartesian point that lies on the circle.
5 .Performing hybrid transformation (translation followed by scaling).
6. Generating an encoded file.
7. Decrypting the encoded file.(using inverse transformations).

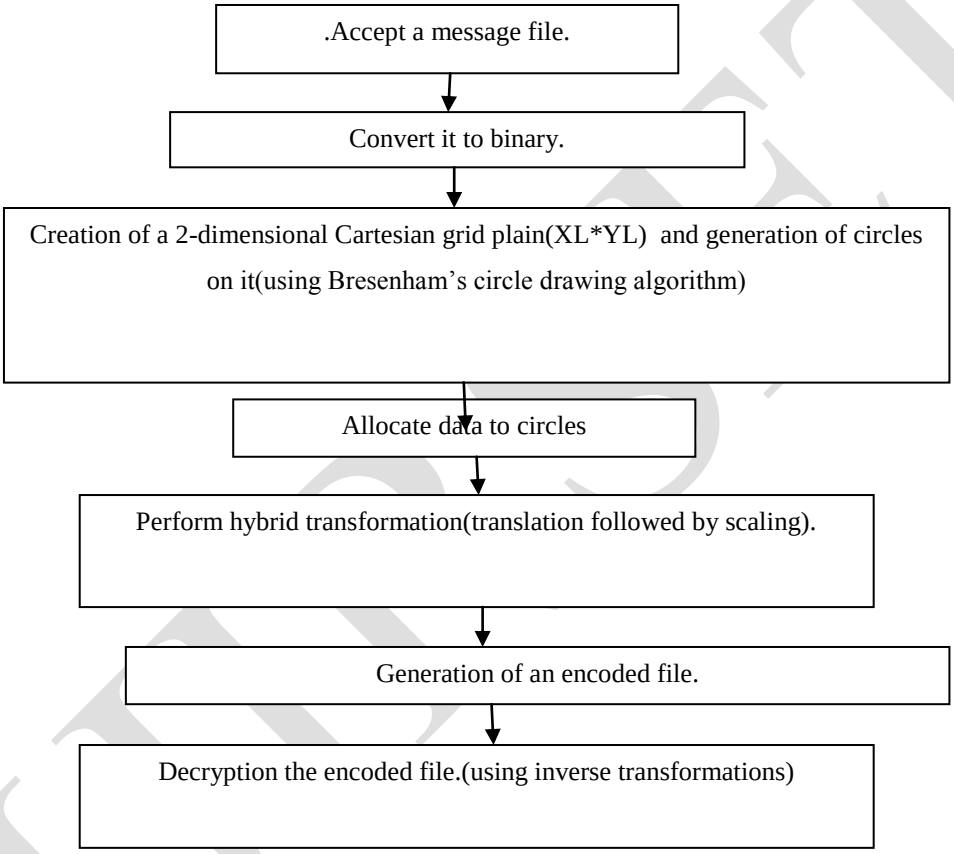



Fig. 3: Flowchart of the proposed algorithm

DOI: 10.15680/IJIRSET.2014.0312083

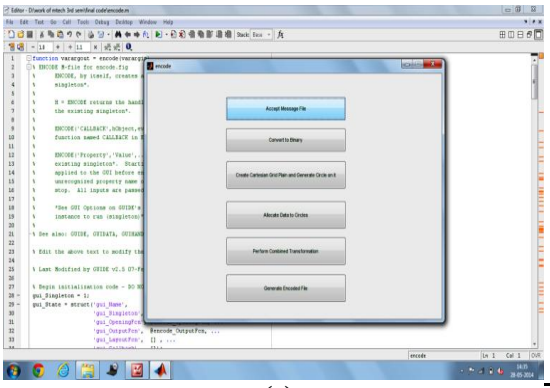
ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

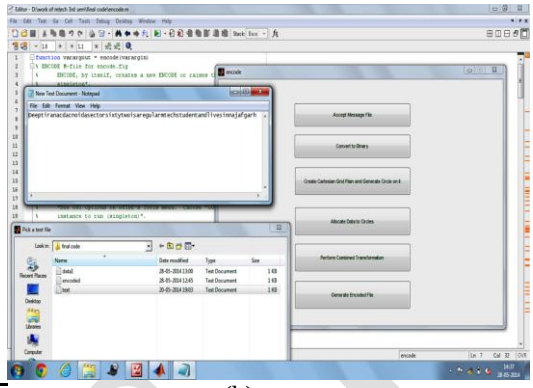
*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

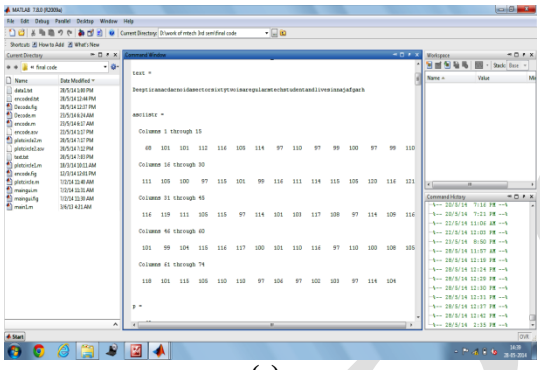
## V. EXPERIMENTAL RESULTS



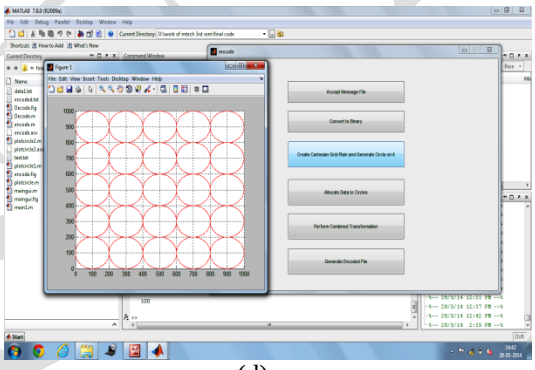
(a)



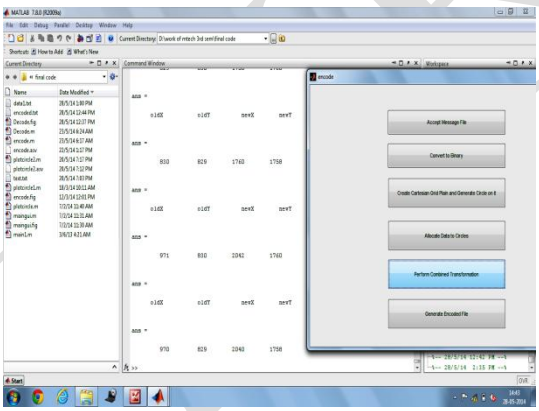
(b)



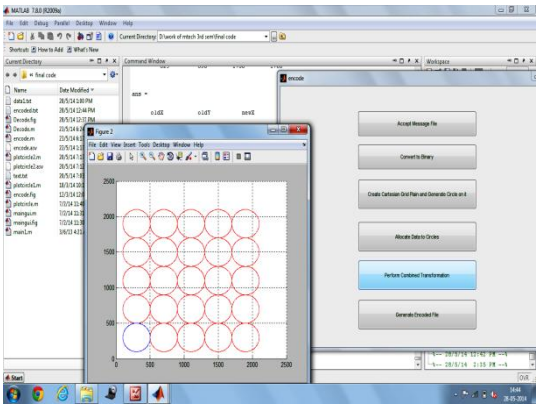
(c)



(d)



(e)



(f)

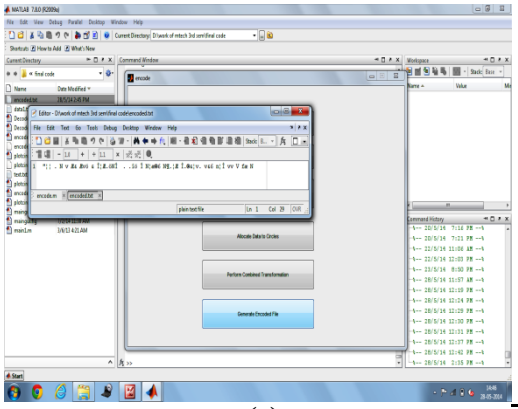
DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

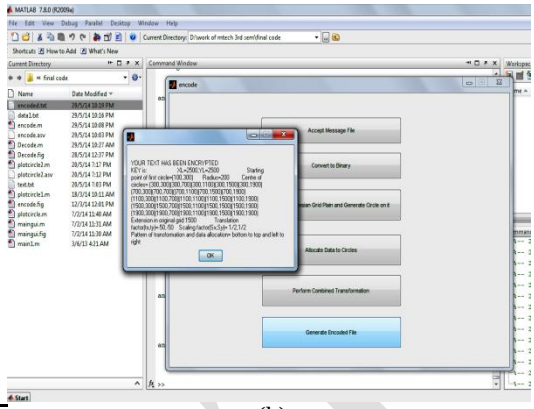
International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

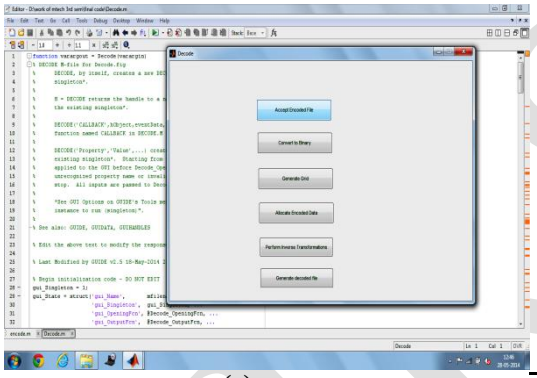


(g)

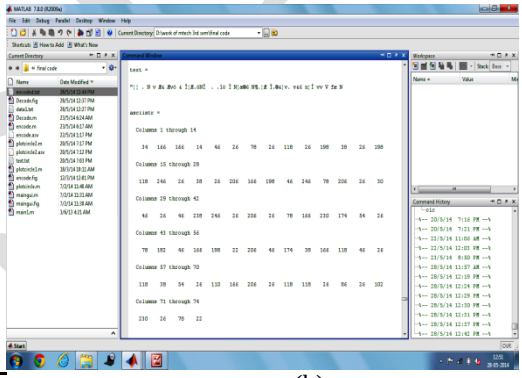


(h)

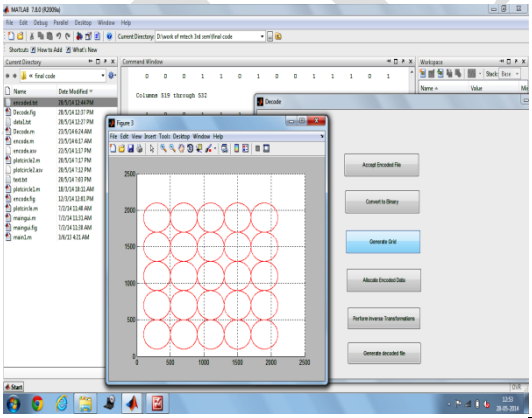
Fig. 4: Encryption (a) GUI for Encryption showing all the steps(b) Accepting a message file (c) Converting the file to binary (d) Creation of 2D data grid and generation of circles over it using Bresenham's circle generation algorithm (e) Performing combined transformation i.e. Scaling followed by translation (f) Grid after performing combined transformation (g) Generation of encoded file (h) Dialog box showing the generated key.



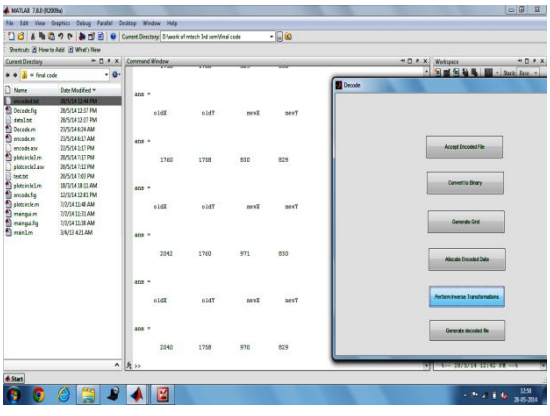
(a)



(b)



(c)



(d)

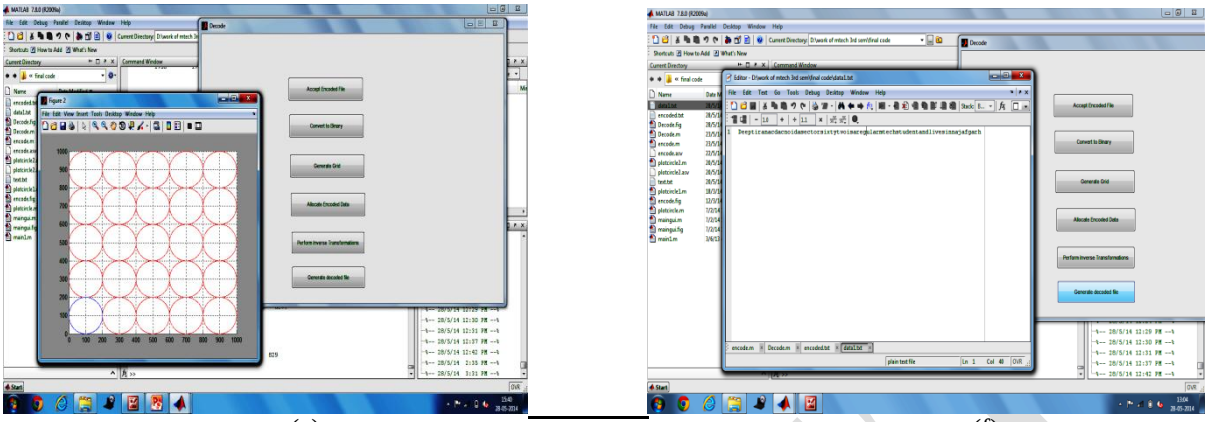
DOI: 10.15680/IJIRSET.2014.0312083

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**



(e) (f)

Fig. 5: Decryption (a) GUI for Decryption showing all the steps (b) Conversion of selected encrypted file to binary (c) Creation of 2D data grid and generation of circles over it using Bresenham's circle generation algorithm, and the parameters given in the key (d) Performing inverse transformation on data using the parameters given in the key(e) Grid after performing inverse transformations i.e. anti translation and anti scaling (f) Generation of decoded text file

As shown in the above figures(Fig 4 and Fig 5), a Cartesian grid plain is generated with dimensions XL=1000 and YL=1000. Circles are generated over it using Bresenham's circle generation algorithm with centre of first circle located at (100,100),(Fig:4(d)) . (0,100) is taken as the reference point or the starting point of data allocation and geometric transformations, for the algorithm to work. A point data type named "location" is used in the algorithm which accepts( X-co-ordinately-coordinate, data value) as its parameter. The data value is always in bit form( 0 or 1). Data in the bits form is allocated to the respective coordinates on the boundary of circles, in the same fashion as the Bresenham's algorithm works. Combined transformations (i.e. translation followed by scaling) are applied over each point on the circle boundary(Fig:4(e)). The scaling factors used are Sx=2,Sy=2 and the translation factors are Tx = 50, Ty = 50. A new grid is generated (Fig:4(f)) after applying transformations over coordinates to compensate the effect of combined transformations. The dimensions of the new grid are (XL,YL) = (2500,2500).After the transformations are applied, a new pattern for data is obtained and converted to the corresponding ascii values, taking 8-bits of data at a time. The encoded form of data is stored in a separate file named as "encoded.txt"(Fig:4(g)).During decryption encoded data in the bits form is allocated to the corresponding locations in the grid.Inverse transformations are applied over each coordinate, shifting it to the original position(Fig:5(d) & Fig:5(e)). Scaling factors used this time are Sx = 0.5, Sy = 0.5 and translation factors are Tx = -50, Ty = -50.

## VI. CONCLUSION

The presented algorithm is an improvement in the basic Chakra algorithm for symmetric key cryptography. This encryption technique adapts combined transformations,(i.e., translation followed by scaling ) of circumference points of every circle by some scaling factor(Sx,Sy) and translation factor(Tx,Ty).Knowing the centers of circles, radius of every circle, starting point (or reference point), dimensions of the Cartesian grid plain(XL,YL), scaling factors and the translation factors used in encryption, pattern of transformations and the new coordinates, the receiver can use the inverse transformations to achieve the plain text at last. There will be no use of sine and cosine functions, in the proposed approach, thus minimizing the probability of precision errors due to irrational numbers.So,the presented work is more effective in terms of accuracy.

## VII. LIMITATIONS AND FUTURE WORK

The presented work uses constant translation and scaling factors for every circle on the grid making it less difficult to decrypt, hence reducing the security factor to some extent .

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 12, December 2014**

Instead of this, different translation and scaling factors (arrays of translation and scaling factors) can be used for each circle in the grid, hence making the encryption process more secure.

## REFERENCES

[1] P.Ramesh Kumar,S.S. Dhenakaran,K.L. Sailaja,P.Saikishore, "*CHAKRA: A New approach For Symmetric key Cryptography*" ,"2012 World Congress on Information and Communication Technologies"(IEEE Journal),2012

[2] Prerna Gaur,Dr. Paramjeet Singh,"Geometry Based Symmetric Key Cryptograph Using Ellipse", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Vol.2, Issue 6",2013

[3] Chowdhury ,M.J.M.,"A New Symmetric Key Encryption Algorithm based on 2-d Geometry","2009 International Conference on Electronic Computer Technology",2009

[4] W.Stallings,"Cryptography and Network Security",Fourth Edition,Prentice Hall,2005

[5] Donald Hearn, Pauline Baker; " Computer Graphics: C version",Pearson Education; 2005

[6] Behrouz A. Forouzan, Data Communication and Networking, 4th Edition, Tata McGraw Hill Company, 2006