Hiding the Data In Encrypted 2-Dimentional Vector Graphics Depending On Inverse Mapping Method for Real Numbers

Mr.P.Bhaskar [1],M.Tech,Assit Prof, M.Srinivas Naveen [2],B.Tech, S.Sai Lokesh [3],B.Tech, C.Sandeep Reddy[4] ,B.Tech
J.Shyam Durga Prasad[5],B.Tech Y.Sai Teja Reddy[6],B.Tech
Department of Computer Science & engineering
Santhiram Engineering College, Nandyal

Abstract: **In several years has been investigated for Reversible Data Hiding in encrypted domain, But it can done by raster images. Then encryption and data hiding are combined together and different parts of image can separately used for encrypt and data hiding. It leads to concerns risk of data leakage is occur when correlation between the plain text part and encrypted part. We proposed a 2D-Vector Graphics scheme the data must be encrypted and represented that graphics in real numbers and stored on cloud and cloud service provider (CSP) can perform the date hiding and recovering the graphics. By using the method of reversible mapping model for real numbers, first it can build the real numbers in reversible mapping model and maps the points in** R^n to 2^s**non intersecting subsets in** R^n**. For an authorized user can access the recovered encrypted graphics. Whereas unauthorized user can obtain the stego encrypted graphics. The experimental result and analysis can be a good balance between security distortion and capacity.**

Keywords: Reversible data hiding, 2D vector graphics, reversible mapping model, cloud service provider.

I. INTRODUCTION

The popular deployment of cloud services are increased the user can needs the privacy and security for the data. In recent years, the encryption can be done by the raster images in reversible data hiding. But the data leakage should be high in correlation between plain text part and encrypted part.

Currently, introducing the scheme of 2D vector graphics which are represents the data in real numbers. When the user data can stored on cloud, the cloud can encrypt the users data and cloud service provider can perform the data hiding, data extraction and recovered encrypted data. By using reversible mapping model the encrypted 2D graphics can represent in real numbers on any host.

II. EXISTING SYSTEM

The RDX in encryption scheme can perform on the raster images, Different parts of image can perform the encryption and data hiding. Two techniques can be used in existing system, cumulative digital image water marking for data hiding and tree structured haar (TSH) for encryption. In that encryption having the most significant bit (MSB) plain of quantitative coefficients and data hiding having least significant bit. It leads risk of data leakage should be high. To solve this issues we can develop two techniques.

1. Vacating room before encryption (VRBE):

The data owner can create vacant room for data embedding before encryption of data and it locates specific position for embedding the secret key. While processing the image the size should be M*N, Where it first moves [L/N] rows of pixel of least correlation in image [L is length of message]. The LSB and Original image location are embedded in other pixel.

2. Vacating Room After Encryption(VRAE):

The sender encrypts the original image then data hiding can embedded by modifying some bits of encrypted image, In that image can locate position to store. In this VRAE having 3 categories:

a).Data extraction in plain text Domain: The encrypted of image can be done with stream cipher mode and data hiding process is carried out by flipping 3 least significant bits of pixel with set. Data Extraction process has first decrypted and (data hiding process)that pixels are divided into 2 groups of data hiding process.

To data can be recovered by calculating and comparing the correlation of 2 pixel sets.

b).Data Extraction in Cipher text Domain: *I*n this every 'n' pixel of image is encrypted by Advance Encryption standard(AES) algorithm in ECB mode and first bit can embedded by replacing original data under the control of a key. In data extraction process, the embedded data can extract with key in cipher text domain.

c).Data Extraction in both Domains**:** By extraction of both domains data using RDH in encrypted image using pseudorandom sequence modulation. In that process, The content owner can encrypt the original image for protection and data hider replace small portion of LSB's of encrypted image with additional data .while decrypting the data it removes the additional data and original data can be recovered.

III. REVERSIBLE MAPPING MODEL FOR REAL NUMBERS:

In this model consist of majorly 3 independent parts,

a) ***Data Encoding*****:** It encodes the data (or) message to increase its fault tolerance or reduce redundancy.
b) ***Embedding Features Selection*****:** This is used to select sufficient features of data hiding and different embedded features can perform of invisibility, capacity and robustness.
c) ***Data Hiding Function*****:** In this part various methods are used to hide the data.

The Reversible Mapping model can be done with Expansion Shifting Model.

A).Analysis of Integer based on general expansion shifting model:

The formula for expansion shifting model is

$$f: Z^n \rightarrow P(Z^n)-\{\emptyset\},\ldots\ldots\ldots\ldots(1)$$

where $P(Z^n)$ is power set of Z^n

To guarantee the reversibility, *f* should satisfy the following property

$$x_1 \neq x_2 \Rightarrow f(x_1) \cap f(x_2)=\emptyset \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Assume $f(x)=\{X_1',\ldots,X_m'\}$, $m=|f(x)|$ represents cardinality of set f(x)

the embedding process done by two situations

1) If M=1,xwillbeshiftedtox[.
2) If M > 1, x will be expanded to one element in f(x).

Calculation embedding capacity

$$EC(f)=\sum_{x \in Z_n} h_{f(x)} \log_2 |f(x)|$$

Calculating total distortion

$$ED(f)=\sum h_{f(x)} \sum_{x' \in f(x)} d(x, x') / |f(x)|$$

Where $h_{f(x)}$ is number of repetitions of x with 'n' dimension of data set

$D(x,y)=||x-y||^p$ represents l^p- normal between x and y

The minimum total distortion can be define when

$$f(t)=\{t-2^{C-1}+1,\ldots,t,\ldots,t+2^{C-1}\}$$

The maximum distortion can be defined

$$Maxd=Max(d_{tr} \in f(t)(t^r-t))=2^{C-1}.$$

The average distorting calculation is

$$1+2^{c-1}$$

$$ED(f)=\tfrac{1}{2}\sum |i-t|=2^{c-2}+1/2^c-1/2$$

$$i=t-2^{c-1}+1$$

B).Reversible mapping model for real number:

The real number is defined as

$$g: R^n \Rightarrow P(R^n)-\{\emptyset\}$$

where g should satisfy the property of equation 2

Unlikely the integer set, The cardinality of real number set in a special interval equals that whole real number. Then assume that whole space is divided into 2^s non-overlap sub-sets. Then satisfy the property as given below

$$\forall x \in R^n, |g(x)|=2^s>1$$

Where s represents embedding strength

Before measuring its distortion and capacity then function $h_{g(x)}$& $h_{f(x)}$ is represents in similar

$$h_g: R^n \Rightarrow z^*$$

S bit can embedded into every element $x \in R^n$

The calculation of total capacity EC(g) is shown below

$$Ec(g)=\int\ldots\int h_{g(x)} \log_2 |g(x)| dx_1, dx_2 \ldots dx_n$$
$$=s\int\ldots\int h_{g(x)} dx_1, dx_2 \ldots dx_n$$

Where $x_1, x_2 \ldots x_n$ represent n dimensions of data

$$N=\int\ldots\int h_{g(x)} dx_1, dx_2 \ldots dx_n$$
$$EC(g)=sN$$

The comparison between expansion shifting model and reversible mapping model is shown below

THE COMPARISON BETWEEN THE PROPOSED MODEL AND [33]

	General expansion-shifting model[33]	The proposed model
Data Format	Integer	Real number
Data Change	Some of x will be expanded into a set with more than 1 element;	Arbitrary x will be expanded into the set with more than 1 element;
Capacity	$\sum_{x \in Z^n} h_f(x) \log_2 \lvert f(x) \rvert$	sN
Lower bound of average distortion	$\overline{ED}(f)=\Omega(2^C)$	$\overline{ED}(g)=O(1)$

IV.PROPOSED SCHEME

RDH in encrypted 2D-Vector graphics ,The distortion between original graphics and data hiding ,after decryption should be small and distributed in large range of data. The little bit work is done by the raster image to represents 2D vector graphics. Based on expansion shifting model we can provide large distortion with stable capacity. The diagram is shown be

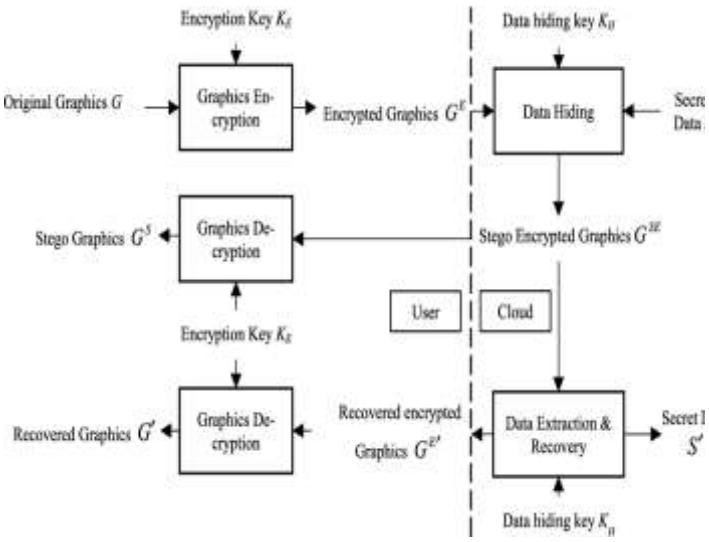


Fig: 1.Frame work of RDH in encrypted 2D vector graphics

After the graphics owner encrypts and upload the graphics to cloud, Then Cloud service provider can hide data into encrypted graphics

In this proposed model having mainly 3 parts

a). Graphics Encryption :

The data of 2D vector graphics can represented in double – precision floating number. The approximately implement of real number. Formula is shown below

$$x = (-1)^{sig}(1.b_{51}b_{50}...b_0)_2 \times 2^{e-1023}$$

where *sig* is a sign bit, $b_{51}b_{50}...b_0$ is the fraction part. *e* is the non-negative exponent part with a length of 11 bits.

The graphics processing software can works on these situations:

- All bits of numbers e are '1',then rendering system will report as error.
- When the bit of number e is equals '0',then fraction part can discarded during data saving.
- When absolute value of number is greater than 10^{100},then number will be set to 10^{100}

Step 1: For a given 2D vector graphic G, extract its vertices and obtain a vertex set

$V = \{v_i | v_i = \{x_i , y_i \}, i \in \{0, ... ,n-1\}\}$.

Step 2: Based on the RANDOMIZE-IN-PLACE program a pseudorandom array $A = \{a_0, a_1, \dots , a_{n-1}$ $(a_i \in \{0, \dots , n-1\})$ is generated under the control of an encryption key K_E

Step 3: The scrambled vertex set of V is $V^A = \{v^A | v^A = \{x^A, y^A\}, i \in \{0,... , n-1\}\}$ is obtained as

$$\mathbf{v^A = v_i.}$$

Step 4: Encrypt the coordinates of the scrambled vertices. Takethex-coordinate x^A as an example, the bits of the fraction part, the sign bit, and the exponent part are calculated as

$$b_{i,k}^A = {}' x^A \cdot 2^{52-k} {}' \bmod 2 (k=51,50,\dots,0),$$

$$sig_i^A = {}' 1/2 - sign(x^A)/2 {}',$$

$$e_i^A = {}' \log_2 x^A {}' + 1023,$$

where sign(.) is function to obtain sign of input and 53 pseudorandom bits $r_i^x = \{r_{i,0}^x, r_{i,1}^x, \dots, r_{i,52}^x\}$ are generated by standard stream cipher with key K_E and used to encrypt is

$$b_{i,k}^E = b_{i,k}^A \oplus r_{i,k}^x \quad (k = 0,1,\dots,51)$$

$$sig_i^E = sig_i^A \oplus r_{i,52}$$

Step 5: Update the encrypted vertex set V^E into the graphics, and the encrypted graphic G^E is obtained.

b).Data Hiding :

For the encrypted co-ordinates values may be very large by that implements the co-ordinates with fixed parameters like 2^S, l, Δ . the simplification of data hiding are represented as follows

$$D = \{d_i / d_i \in \{0,1\}, i \in \{0,1,\dots,L-1\}\}$$

Where L=2N*S, N is number of vertices in graphics

S is an embedding strength

Step1: Encrypt D with a stream cipher and data hiding key K_H and obtain D^E.

Step2: Segment D^E into groups with a length of S-bits and $W = \{w_i | w_i \in \{0, 1, \dots , 2^s - 1\}, i \in \{0, 1, \dots , 2N - 1\}\}$ is obtained.

Step 3: Extract the vertices of the encrypted 2D vector graphic G^E , and a vertex set V^E is obtained.

Step 4*:* The first *sN* elements of *W* are embedded into the *x* -coordinates of V^E orderly by

$$x_i^{SE} = [x_i^E / 2^{e_i^E-1023-t_i}] * 2^{e_i^E-1023-t_i} + w_i * 2^{e_i^E-1023-t_i} / 2^S + x_i^E - [x_i^E / 2^{e_i^E-1023-t_i}] / 2^S$$

Step 5: In the same way, embed the rest data into the y-coordinates of V^E .

Step 6: Update the stego encrypted vertex set V^{SE} into the graphics and obtain the stego encrypted graphic G^{SE}.

c).Data Extraction and Graphics Recovery:

It must be done by inverse process of data hiding

Step 1: Extract the vertices of the stego encrypted graphics G^{SE} and obtain a vertex set

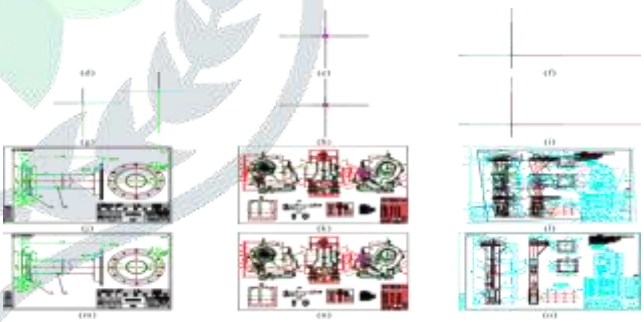
$$V^{SE} = \{ V^i / V^i = \{x_i, y_i\} \; i \in \{0,..,N-1\}\}$$

Step2: Extract the hidden data segment from x and y co-ordinates V^{SE} as

$$W_i^1 = [x_i^{SE} / 2^{e_i^E-1023-t_i-s}] - [x_i^{SE} / 2^{e_i^E-1023-t_i}] * 2^S$$

Step 3: Concatenate the hidden data segment and obtain the encrypted data D^1E.

Step 4: Decrypt D^1E with K_H and obtain original data D^1.



Step 5: Recover the x co-ordinates of V^{SE} is

$$X_i^{1E} = (x_i^{SE} - [x_i^{SE} / 2^{e_i^E-1023-t_i-s}] * 2^{e_i^E-1023-t_i-s}) * 2^S - W_i^1 * 2^{e_i^E-1023-t_i-s} + [x_i^{SE} / 2^{e_i^E-1023-t_i}] * 2^{e_i^E-1023-t_i}.$$

Step 6: Update the recovered vertex set V^{1E} into graphics and the original encrypted graphics G^{1E} is recovered.

d).Graphics Decryption:

The decryption can be done by inverse of encryption, Then authorized user can obtain the original encrypted graphics G^{1E}& un-authorized user can obtain the stego encrypted graphics G^{SE}.

Step 1: Extract the vertices of $G^{r(S)E}$ and obtain the vertex set $V^{1(S)E}$.

Step 2: Generate a pseudorandom array $A\{a_i | a_i, i \in \{0,1,..,n-1\}\}$ under the control of K_E.

Step 3: Decrypt the vertex $v_i^{r(S)E} = (x_i^{r(S)E} , y_i^{r(S)E})$

$$b_i^{r(S)\,A} = b_i^{r(S)E} \oplus r_{i,k} \; (k = 0, 1, \dots, 51),$$

$$sig_i^{r(S)\,A} = sig_i^{r(S)E} \oplus ri,52.$$

Step 4: Inverse scrambling is done to the elements of the vertex

Step 5: Update the decrypted vertices into the graphics and obtain the decrypted graphics $G^{1(S)}$.

V. Experimental results:

The experimental can be done by pc with configuration is : CPU i5-4460S 2.90 GHz, RAM 16 GB, Windows 7 64bit,DWG direct C++ Libraries, and Visual C++6.0.Graphicsencryption,datahiding,dataextraction,and graphics decryption are all done to 50 2D engineering graphics, The parameters for the experiments are: embedding strength $s = 2$, $a = 4$, $b = 10$,$MaxExp = 1350$,

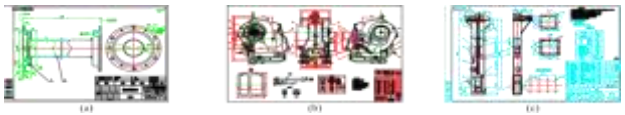


Fig. 2. Experimental results of some sample 2D engineering graphics. (a)–(c) Original graphics. (d)–(f) Encrypted graphics. (g)–(i) Stego encrypted graphics. (j)–(l) Decrypted stego graphics. (m)–(o) Recovered graphics.

Table 1: Details of Test Graphics

Graphics	Vertices number	Feature number
G1	232	175
G2	5716	3385
G3	1961	1165
G4	1465	931
G5	3611	2238
Average of 50 graphics	3829.44	2113.84

The above table results indicates that

I. The distortion between encrypted graphics and original graphics are very large.
II. This method can correctly extract the hidden data.
III. The distortion between decrypted stego graphics and original is small.

Calculating the Average distortion by using the formula

$$\text{Avg } D(V,V^1) = 1/N \sum_{i=0}^{N-1} \|v_i - v_i^1\|$$

Calculation the maximum movements by using the formula

$$\text{Max } D(V,V^1) = \max(\|v_i - v_i^1\|),\ i \in \{0,1\ldots,N-1\}$$

The difference of original graphics and recovered graphics having the good reversibility as shown table.

Table 4

Graphics	*AvgD*	*MaxD*
G1	7.1803×10^{-14}	3.4224×10^{-13}
G2	2.1254×10^{-13}	7.6263×10^{-13}
G3	2.5934×10^{-12}	5.6249×10^{-12}
G4	1.2838×10^{-13}	4.6874×10^{-13}
G5	5.4364×10^{-14}	2.4117×10^{-13}
Average of 50 graphics	2.7754×10^{-13}	9.0404×10^{-13}

VI. ANALYSIS:

a). Analysis of Capacity:

By analyze the capacity the hidden s bits/vertex into every x and y co-ordinate, If the number of vertices of a graphics is N and its total capacity is 2Ns bits, The average capacity is 2s bits/vertex.

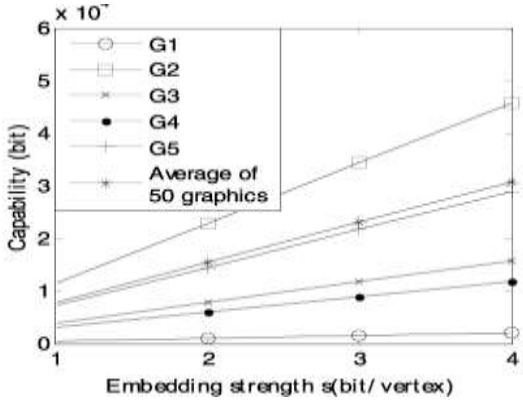


Fig: 3.The relation between capacity and embedding strength s.

The Figure shows that increasing both capacity and its embedding strength s.

The capacity of past scheme and proposed scheme is shown table

Table 2: Comparison of past scheme and proposed scheme

Graphics	urDEED[8]	Proposed
G1	0	928
G2	8	22864
G3	4	7844
G4	6	5860
G5	8	14444
Average of 50 graphics	8.36	15317.76

It shows the good capacity strength compared to past scheme

VII. CONCLUSION

By using this scheme, the encrypted data can represent by 2D vector graphics to improve the encrypted security and high capacity. The Experiment results should be good results and based on model, the reversible mapping model for real numbers is suitable for represents any host in real numbers. Theoretically analysis proved that embedded strength and capacity is increased relatively.

VIII. FUTURE ENHANCEMENTS

Furthermore, the distortion between the decrypted stego graphics and the original ones can be controlled by adjusting the parameters. It provides a possible means for the management of encrypted vector graphics in cloud manufacturing.