ISSN: 0067-2904

Image Encryption Based on Intelligent Session Mask Keys

Hala Bahjat AbdulWahab
Department of Computer Science, University of Technology, Baghdad, Iraq.

Abstract

The revolution of multimedia has been a driving force behind fast and secured data transmission techniques. The security of image information from unapproved access is imperative. Encryptions technique is used to transfer data, where each kind of data has its own special elements; thus various methods should to be used to conserve distributing the image. This paper produces image encryption improvements based on proposed an approach to generate efficient intelligent session (mask keys) based on investigates from the combination between robust feature for ECC algebra and construction level in Greedy Randomized Adaptive Search Procedure (GRASP) to produce durable symmetric session mask keys consist of ECC points. Symmetric behavior for ECC by keeping the points set Ps as 1D mask secret key produce. B^+ tree compress operations use to increase the security level and reduce multi session secret mask keys size based on indexing data base to unique code that transmit between the sender and receiver in secure channel. According to the popular measurements the proposed approach give efficient results in image encryption and the proposed method to generate 1D intelligent mask generation succeed to conceal pure images information.

Keywords: Digital image processing, ECC Algebra, *GRASP* algorithms and *B+ tree*.

التشفير الصوري بالاعتماد على مفاتيح الجلسات الذكية

هالة بهجت عبد الوهاب

قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة

أن ثورة الوسائط المتعددة تشكل دافع قوي وراء تقنيات نقل البيانات السريعة والمضمونة كما اصبحت حماية بيانات الصورة من الوصول الغيرمصرح حاجة ملحه. تقنيات التشفير لنقل البيانات لها سماتهاالخاصة، لذا دعت الحاجة الى أستخدام أساليب مختلفة لحماية الصورة السرية. هذا البحث يقدم تحسين على تشفيرالصور من خلال اقتراح طريقة جديدة لتوليد مفاتيح جلسات ذكية بالأعتماد على دمج بين الميزات القوية لجبر تشفير المنحني الاهليجي ECC ومستوى البناء في خوارزمية GRASP لتوليد مفاتيح جلسات متماثل مؤلفة من نقاط ECC . نهج التشفير المتماثل عن طريق الحفاظ على نقاط ECCبصيغة mask keys تم أعتماده. ان عمليات الضغط لهيكل الشجيري B^+ أستخدم في هذا البحث لبناء قاعدة بيانات مفهرسة للمفاتيح الجلسات الذكية وكذلك لزيادة مستوى الامنية وضغط حجم العديد من مفاتيح الجلسات الى رمزفريد لارساله في قناة امنة بين المرسل والمستلم.وفقا للمقاييس الشائعه ان النهج المقترح اعطى نتائج كفوءة في

Email: hala_bahjat@yahoo.com

تشفير الصورة والطريقة المقترحة لتوليد mask keys ذكي احادي الابعاد نجحت في إخفاء المعلومات الصور النقيه.

Introduction

The late improvement in personal computer manufacture and correspondences make a business opportunity for computerized mixed media appropriation through open system networks. In open system networks, privacy is one of the essential attentiveness toward business employments of interactive media substance. The common case of organized sight and sound implementations are video on interest, net, TV, video communication, and video conference. These species of utilizations demand a kind of security; for instance, in the application of video conference just the taking an interest individuals are permitted to get the sound and video information, and in the application of video on request only the video owners might want just the supporters to watch the high quality of video [1].

Littler and speedier protection algorithms give portion of the arrangement, the elliptic curve cryptography ECC give a quicker other option to cryptography of public key type. In this type the small key lengths are essential with ECC to give a sought grade of security, whose implies fast exchanging of key, generating of signature and verification, client authentication, the storage memory that needs of ECC key is very small. The ECC cryptography and ciphering alludes to a current nonspecific cryptosystem which utilize codes produced from an elliptic curve [2].

Greedy Randomized Adaptive Search Procedure (GRASP) is a met heuristic strategy commonly added in successful to different combinative optimized problems [3-6]. A GRASP is peatedrestraint, where every GRASP reiteration has of two parts: structuring and local seeking. The structuring part is the greedy strategy utilized to establish a practical resolution. The second part is a local seeking which is utilized to totalize the result institute by the first part of the GRASP strategy. The two parts are refined different case unaided or by use a confirmed learning procedure and the better result is chosen as the end results. So as to gets an optimized problem by using a GRASP strategy [6].

The met algorithm of heuristic which applied effectively to a few combinatorial enhancement issues that called by Greedy Randomized Adaptive Search Procedure (GRASP) [3-4-5-6].These is an iterative strategy, where every iteration of GRASP comprises of two stages: first is construction stage, second is local stage. The first stage is eager strategy utilized to assemble a clear result where in the second stage which is utilized to improve the arrangement construct by the first stage of the GRASP method. The two stages are refined a few cases autonomously or utilizing a specific learning strategy and the better general solutions is chosen as the last results. Keeping in mind the problem is optimization by utilizing a GRASP methodology [6].

This paper produces an idea for an application for GRASP procedure to generate intelligent session mask keys based on ECC algebra with symmetric behavior by keeping the points set Ps as 1D mask secret key .B+ tree compress operations use to increase the security level by reduce the secret mask key size in transmit stage between the sender and receiver in secure channel.

Algebraic Description of Addition operation

This section illustrates the calculation additions over elliptic curves that used in this paper. For two different points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ that are not negatives of each other, the slope of the line *l* that joins them is: $\lambda = (y_Q - y_P) / (x_Q - x_P)$.There is also one other point where *l* intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic modification, one can refine the sum R = P + Q as follows: [7]

$$X_R = (\lambda^2 - X_P - X_Q) \bmod p \quad \ldots\ldots (1)$$

$$Y_R = (\lambda (X_P - X_R) - Y_P) \bmod p$$

That is indeed to be able to sum a point to itself: P + P = 2P = R. When $y_P \neq 0$, the equations are:

$$X_R = \left(\frac{3Xp^2+a}{2Yp}\right) - 2Xp \quad \ldots\ldots (2)$$

$$Y_R = \left(\frac{3Xp^2+a}{2Yp}\right)(Xp - Xr) - Yp$$

In cryptographic applications, two families types of elliptic curves utilized, prime curves over Z_p and binary curves over GF (2^m). For a prime curve over Z_p, a cubic equation will be used in which the variables and coefficients all occupy on amount in the set of integers from 0 to p - 1 and in which

accomplish based on modulo p. A binary curve defined over GF(2^m), the variables and coefficients all occupy on amount in GF(2^n) and in computations are accomplish over GF(2^n) [8].

Construction phase description

The Met heuristic Greedy Randomized Adaptive Search Procedure (GRASP) is a multi-start iterative process, in which each round has two parts: first phase is structure and second phase is local investigation. Structure phase starts from a flatulent result, full solutions are structured in iteratively by one variable at a time. At every structure refinement, the preference of the following variable to be added is resolved by organizing all nominee variables is a nominee listing *C* with regard to a greedy function *g*: *C*→*R* [9]. This function gauges the interest of choosing each variable.

The heuristic is adaptive because the avail correlating with each variable are changed from the origin at each round of the structure part to invert the alteration transported on by the chosen of the former variable. The probabilistic part of a GRASP is described by random selecting of one of the better nominee in the listing, but not needs the top nominee. The listing of better nominees is said the restricted candidate list (RCL) [9].

The GRASP Met heuristic is an iterative procedure of multi start, in which every iteration comprises of two stages: first stage is construction and the second stage is local search. First stage begins from an unfilled arrangement; a complete arrangement is iteratively built by one component at once. At every iteration of construction, the following variable chosen to be insert is dictated by arranging all competitor components in an applicant list C concerning a greedy function g :C→R.

This procedure menstruations the interest of choosing every component. The heuristic is adaptive in order that the advantages supported with each component are overhauled at every round of the first stage to mirror the alterations transported on by the determination of the prior component. The probabilistic part of a GRASP is described by arbitrarily selecting one of the best applicants on the list, yet not as a matter of course the top candidate. The best nominee is known as the restricted candidate list (RCL). Algorithm (1) illustrated the basic GRASP construction stage [10].

Algorithm (1): basic GRASP construction
Input*: assume s=0%* where *s* is a fractional result in this situation *and*
α= represent as List Length () of Candidate % RCL length.
Output: Restricted candidate list (RCL)
Process:
Step-1: do
Step-2: Generating the Restricted Candidate List(*s*) and put into *RCL* of (α)
Step-3: x is equal the value of Selecting random Element of *RCL*(α)
Step-4: Lets value is equal the $s \cup \{x\}$Update Greedy Function(*s*) % update of the heuristic amounts updating
Step-5: While solution not complete go to step-1
End

B^+ Tree

B^+ tree called an indicator of database (DB), that every register will be saved in the DB, the indicate no. (The clef) of that register will be saved in the B^+ tree. Therefore when one needs to arrive a confirmed register, one requires to inform its key to bring it's indicate no. from the B^+ tree. When one bring the indicate no. of that register one can restore the desired register immediately. B^+ tree is coordinate and stable tree that shown in Figure-1 and this is why it is so rapid in restoring the desired information. B^+ trees recognize inside and leaf nodes, conservation information just at the leaves, while customary B^+ trees would likewise storage the clefs in the inside. B^+ tree enrolment, consequently, demands dealing with the inside node reference amount notwithstanding just returns a stain for the information, as in the easiest B-tree strategy [11, 12].

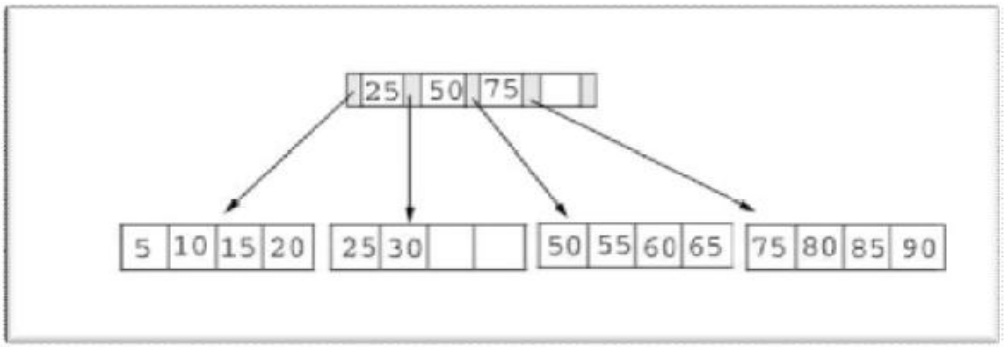

Figure 1- B^+ Tree example.

B^+ tree utilized as a particular vocabulary for saving information with their symbol in a method that prohibit redundancies of these information or even sub information in this vocabulary (so as to supply effective memory employment), with conformity to the dependent status [13]:

1. Save information in this vocabulary (if it is not point) and bring its unrivaled symbol (at transmit operation).
2. Restore the unrivaled information when one has its symbol from this vocabulary (at received operation)

B^+ tree transforms the key to little symbol no's by probing from the compressing feature that obtainable in B^+ tree construction (indicating construction), that was operative in a method that prohibit redundancies of these key or even sub key orderly to supply effective memory use. This phase exemplifies by saving the one or more keys and bringing its singular number based on B^+ tree indicating, so as to extent singular numbers for every key [14].

Proposed Approach

Secrete session intelligent mask key algorithm produce based on the proposed combination between the robust feature for ECC algebra, intelligent features that provided in GRASP algorithm and B+ tree compression operations. The key generation process consists of four stages. First stage represent by generate all possible ECC points (key space generation), second stage represent by Gasp algorithms - construction phase that used as generator to multi mask session keys according base point by investigate from the iteration operations that grasp algorithm - construction phase provided , third stage is compression stage using B+ tree operation in order generate symmetric and secure indexing database for all the session mask key that generated and to increase the security level by convert the mask key to unique code that send with encrypted image same as Pretty Good Privacy (PGP) cryptography protocol behavior. Finally is encryption stage based on ECC addition algebra between the 1D session mask key and secure digital image . In the following illustrated the secret information that pr-agreement between the authorized parties:-

1. Choose big prime number that represents the key space and parameters ECC parameter P, a and b that per-agreement between authorized sender and receiver.
2. Agreement between the sender and receiver to the mask size.
3. Build symmetric B+ tree indexing database for session mask keys based on Gasp algorithms - construction phase.

In the following Figures-2 and 3 illustrated the main descriptions for the proposed approach to generate the secrete session intelligent mask, sending process and receiving process.

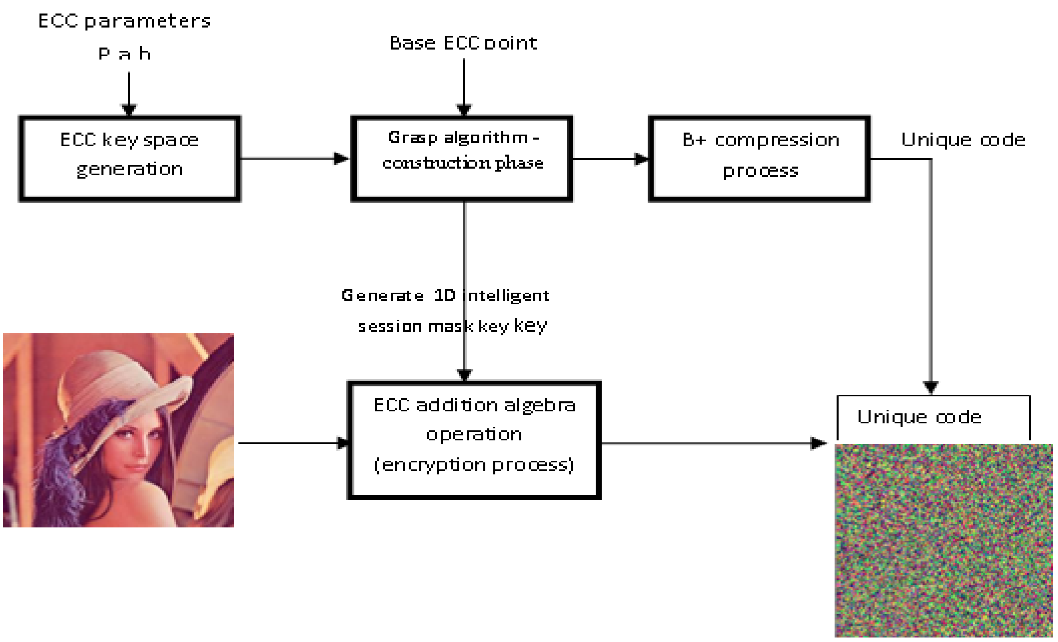

Figure 2- The proposed approach to generate the secrete session intelligent mask and sending process

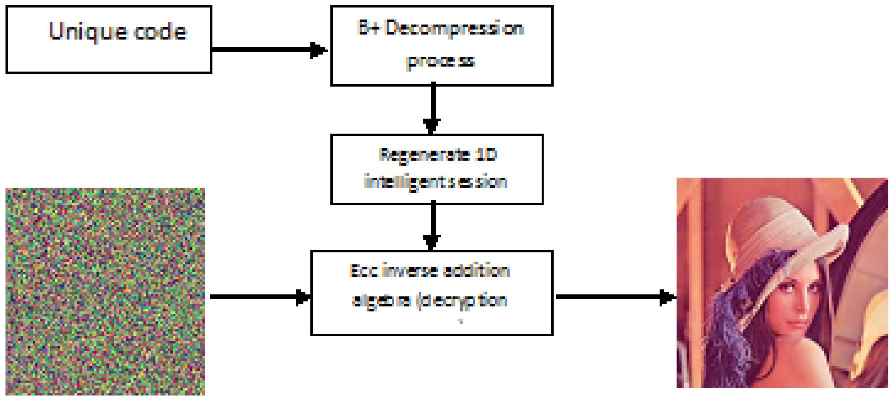

Figure 3- The proposed approach to regenerate the secrete session intelligent mask key and receiving process.

Generate ECC point (key space generation) stage

1. Create the 1D mask depending on the arithmetic of EC algebra, by taking the numbers (0 to P-1) and apply the following eq-3:

$Y^2 \bmod P = (X^3 + aX) \bmod P$ ……………………………………………………………...…..(3)

Ordered pair (x,y) was created from the number of pairs depending on the size of the mask keys.

2. Compute cost for ECC points based on Elliptic Curve Discrete Logarithm (k), which represent the contents of candidate list(C) that satisfy the condition k >0 .

Note:-ECC Discreet Logarithm (*k*) is calculated by this eq-4:

$kP = Q$ ....(4)

Where: P is the base point and *k* is discreet logarithm of Q point

Construction Phase (intelligent generator) stage

The proposed approach produce the Grasp algorithm- Construction as intelligent generator to generate the multi 1D mask keys based on ECC base point, where the sender select one of them for each session, according the following steps :

Step-1: Select the ECC base point randomly

Step-2: Construct Restricted Candidate List(RCL) with Value-Based (VB) mechanism in the following eq-5- to determine maximum feasible solution :

$\mu = gmin + \alpha(gmax - gmin)$ ……..……..…..…(5).

Where:

- α a parameter $\in$ [0, 1], the case α = 0 corresponds to a pure greedy algorithm, while α = 1 is equivalent to a random construction.
- *gmin* and *gmax* be the smallest and the largest incremental costs, respectively.

Step-3: Select random point from RCL list :-

If (the selected point exists in the previous that stored in RCL_DB)

Then (make it as new Base point in the next iteration).

Else (Return to step2).

Step-4: Update candidate list (C)

Step-5: Return to step-3to regenerate a new base point,,

Step-6: Repeat the procedure (step-3…step-6) until reach to length of key mask that agreement.

Compression stage

According agreement between the sender and receiver to build a symmetric B+ tree indexing database for all GRASP algorithm solutions to produce the session mask keys base on pre-agreement to the secret large prime number (p) and the secret parameter (a, b). The compression stage represents by following steps:-

Step-1: Converting the multi session mask keys to unique code was performed through the sending process.

Step-2: The B+ tree algorithm utilizes one DB that exemplifies the dictionary of the session mask key positions and its conformable symbols, and utilizes two indicate trees (Bt1, Bt2) that indicate to the self same DB.

Step-3: Each novel session mask key (attitude) will be transformed into a list of words and these words will be saved in DB in a method that prohibit the redundancies of these places or even sub places.

Step-4: Bt1 is utilized for saving objective to examine if the column of places or even sub places are formerly set in DB. So Bt1 utilize the first situation of the column as a key, while Bt2 is utilized for restoring objective, so it utilizes the symbol of the place the key. In general the session mask key is collected by [w1, w2, wn] where w mean word.

Encryption stage

Passing the intelligent 1D mask key along the pixel's content of digital image using the color represent as(x, y) for each pixel in order implement ECC addition algebra operation , by separate the color pixels(RGB) to red ,green and blue and save colors(R,G,B)in one-dimension array (pic1). In the following an algorithm (2) that illustrates the converting the RGB colors to one-dimension array.

Algorithm (2): convert (RGB) as a vector.
Input: Assume the initialization values for the parameter count=0 and pixel=0
Output: Converting the RGB colors to one-dimension array (pic1).
Process:

```
For i = 0 to height of Digital secure image
For j = 0 to width of Digital secure image
pixel = Picture1.Point(i, j)
Red = pixel& Mod 256  { separate the  Red color values }
pic1 (count) = Red
count = count + 1
Green = ((pixel& and &HFF00FF00) / 256&) Mod 256&  pic1(sum) { separate the
        Green color values }
Blue = (pixel& and &HFF0000) / 65536 {separate the Blue color values}
count = count + 1
pic1 (count) = Blue
count = count + 1
Next i
Next j
End.
```

Implementation and experimental results

A group can be defined based on the set E(a, b) for specific values of a and b in equation -3, provided the following condition is met according equation-6:

$(4a^3 + 27b^2) \bmod p <> 0 \bmod p$ …….. .(6)

To simplify the process of creating the intillgent session mask key, assume image size (256×256), let the prime number will be (p=251), (a=1 and b=1) .The set of finite numbers that will be used in key generation (0 – p-1) = (0 - 251):

Z_{251} = {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,……...,250}.

The ordered pairs obtained from (p=251) is 281 pairs, some of the ordered pairs points= {(0,1),(0,250),(1,76),(1,175),(3,28),(3,223),(4,123),(4,128),(5,70),(5,181), (7,10), (7,241), (9,57), (9,194),(10,42),(10,209), (11,29), (11,222), (14,91), (14,160), (20,95),(20,156), …..,(246,97), (246,154), (248,67), (248,184)}.

- Let base point P = (3,28).

When P= (3,28), Q_1=(248,67)
2P=P+P=(3,28)+(3,28) =(57,196)
3P=2P+P= (57,196)+(3,28) = (39,226)
4P=3P+P =(39,226)+(3,28)=(112,52)
.
.
214 P=(174,100) + (3,28)= (248,67)

- Discrete logarithm k between (3,28) and (248,67) = 214
- Key space (Q_n) ={(0,1),(248, 67),(0,250),(1,67),(7,241)(4,123), (4,128),(5,70) ,(1,175),…}

The number of ordered pairs different for each prime, choosing from these ordered pairs to fill the secret mask. When using the ordered pair (x,y) in encryption process, inverse of the same ordered pair will be used for decryption process (x, - y). For example the point (0,1) the inverse operateion represent by (0, (-1 + p) mod p)=(0, (-1 + 251) mod 251) = (0,250).When the ordered pairs using to full the encryption mask are={(0,1),(248, 67),(0,250),(1,67),(7,241)}, then the decryption mask (inverse mask) will be {(0,250),(248,184),(0,1),(1,184),(2,10)} that illestrated in Table -1.

Tabel 1- Create inverse mask

Original ordered pairs	Inverse ordered pairs
(0,1)	(0, (-1 + 251) mod 251) = (0,250)
(248,67)	(248, (-67 + 252) mod 251) = (248,184)
(0,250)	(0, (-250 + 251) mod 251) = (0,1)
(1,67)	(1, (-67 + 251) mod 23) = (1,184)
(2,241)	(2,(-241+251) mod 251)=(2,10)

B+ tree compression operations illustrated in the following implementation:
Let the Mask key that want to send={(0,1),(248,67),(0,250),(1,67),(2,241)}

(0,1)→ 00001 word ([ind (0,1),00011,~0,0,1)])
00010 word ([ind (284,67),00011,00001,0,0)])
00011 word ([ind (0,250), 00100, 00001,0,1)])
00100 word ([ind (1,67), 01000, 00011,0,1)])
01000 word ([ind (2,241), ~0,00100,(0,1)]) -------- 1

Figure 4- a,b and c show the experimental results for the proposed approach using digital bitmap image size(256×256) ,and intelligent mask key size=5 with prime number P=251. Popular measurements test are use (MSE, PSNR, SNR and Similarity), Table -2 shown the experimental results measurements.

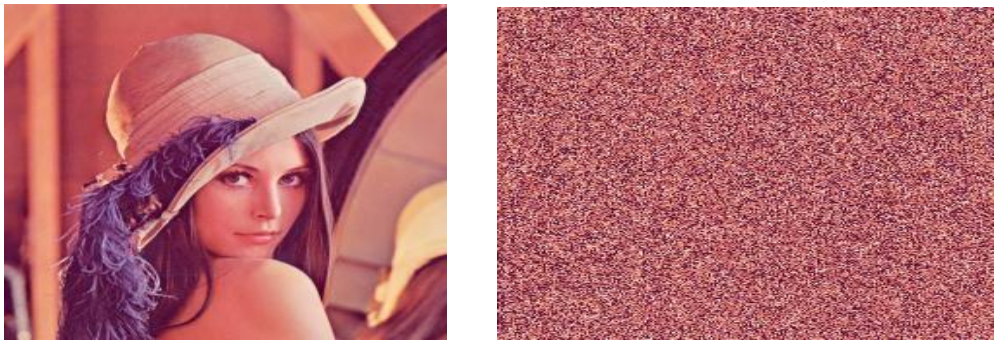

Figure 4a- Original and encrypt lina image size (256×256).

Figure 4b- Original and encrypt car image size (256×256).

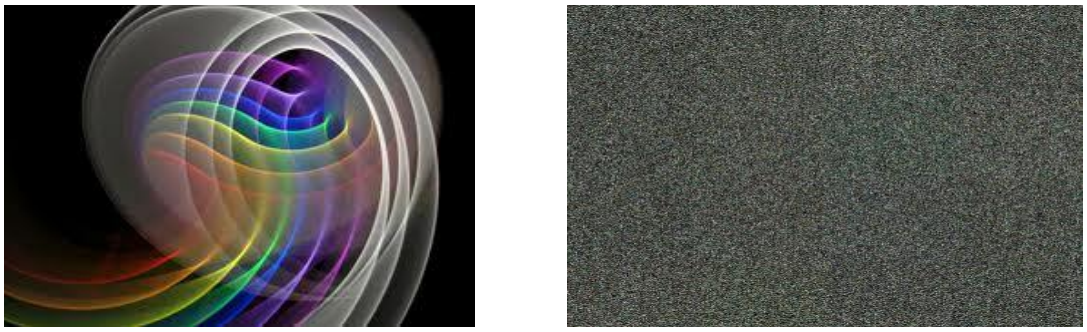

Figure 4c- Original and encrypt waves image size (256×256).
Figure 4 a,b,c- Experimental result for the proposed approach.

Table 2- Experimental results for popular measurements using mask key=5, p=251, a=b=1.

Image size (256×256)	MSE	SNR	PSNR	Similarity
Lena	7181.3633	3.31404	10.53589	0.8374
Car	8443.4566	0.988736	9.85836	0.82196
Waves	310.0466	0.97865	13.2403	0.90676

According Table (2) we canceled the following results:-

1. The MSE measure test gives high results for images, where SNR and PSNR measures test give low results.
2. According to the confidently scheme measurement the proposed approach give efficient results in image encryption and the proposed method to generate 1D intelligent mask generation succeed to conceal pure images information**.**
3. The similarity measure test shows the amount of correlation between the original secure digital image and ciphered digital image and the result from this test is acceptable.

Conclusions

1. Combine the robust feature from the ECC algebra and the randomize that available in construes-phase in GRASP algorithm to produce efficient results to generate symmetric intelligent 1D session mask keys.
2. The Grasp algorithm with construes phase only that proposed in this paper add a new application to Grasp algorithm as random generate for session key based on change base point for each sending process.
3. B+ tree provide efficient indexing database for all session intelligent 1D mask keys and compression operation that provided in B+ tree play important role to compress the session mask key to unique code and send as session mask key to receiver party.

References

1. Liu, F., Koenig, H. **2010.** A survey of video encryption algorithms. *Computers& Security*, **29**(1): 3–15.
2. DeWinand, B., Preneel. **1998**. Elliptic curve public-key cryptosystems – an introduction. State of *the Art in Applied Cryptography*, LNCS 1528, pp: 131-1411.
3. Luis, M., Salhi, S. and Nagy, G. **2011**. A guided reactive GRASP for the capacitated multi-source Weber problem. *Computers & Operations Research*, **38**(7): 1014-1024.
4. Montoya-Torres, J. R., Aponte, A., Rosas, P. and Caballero-Villalobos, J.P. **2010**. Applying GRASP metaheuristic to solve the single-item two-echelon uncapacitated facility location problem. *International Jounal of Applied Decision Sciences*, **3**(4): 297 – 310.
5. Moura, A.V. and Scaraficci, R.A. **2010**. A GRASP strategy for a more constrained School Timetabling Problem. *International Journal of Operational Research*, **7**(2): 152 – 170.
6. Abdesslem, L. and Sara, C. **2012**. A Novel GRASP Algorithm for Solving the Bin Packing Problem. *International Journal of Information Engineering and Electronic Business*, **2**: 8-14.
7. Stallings, William. **2005**. *Cryptography and Network Security Principles and Practices*. Fourth Edition, Prentice Hall, November.
8. Aydos, Savas and C.K. KoV.**1999**. Implementing network security protocols based on elliptic curve cryptography. 4th Scientific Conference, Symp. Computer Networks, pp:130-139.
9. Feo, T. and Resende, M. **1995**. Greedy randomized adaptive search procedures. *Journal of Global Optimization*, **6**: 109–133.
10. Blum, Christian. and Andrea, Roli. **2003**. Metaheuristics in Combinatorial Optimization. Overview and Conceptual Comparison, *Journal of ACM Computing Surveys* (CSUR), **35**(3): 268-308.
11. Jannink, Jan. **1995**. Implementing Deletion in B+ Trees. *ACM Sigmoid Record*, **24**(1): 33-38.
12. Gotez, Graefe. **2006**. B-tree indexes interpolation search, and skew. In *DaMoN*, Chicago Iiinois,USA.
13. Suhad, M. **2010**. Using B+ Tree to represent secret Massage for steganography purpous. *Journal of Engineering and Techology*, **28**(15): 5102-5112.
14. Abdul Wahab, H. B. **2015**. New Watermark Technique Based on B+ Tree and Mathematical Morphology. *Al-Mustansiriyah Journal of Science*, **26**(1): 92-104.