

## Arabic Language Script Steganography Based on Dynamic Random Linear Regression

Assist.prof. Dr. Hanaa M. Ahmed  
[salmanhanna2007@yahoo.com](mailto:salmanhanna2007@yahoo.com)

Maisa'a Abid Ali khodher  
[maisaa.ali2007@yahoo.com](mailto:maisaa.ali2007@yahoo.com)

**Computer Science Department, University of Technology, Baghdad, Iraq**

### ***Abstract:***

In this research, I have process a problem for all previous methods used to hide information within texts. It is possible attack on them easily. But when I used method of concealment using kashida or cancel kashida. In order to prevent the attack it, in this method. In this research is offer in a new method and to use two levels to hide, the first level is hiding by embedding and addition but the second level is hiding by injection. The first level is embed a secret message one bit in the LSB in the FFT and the addition of one kashida. Using DRLR is NRG to find position that are hiding within the text. The second level is the injection one or two random kashida within the text.

Linguistic steganography is covering all the techniques that deal with using written natural language to hide secret message. in this research presents a linguistic steganography for scripts written in Arabic language, using kashida and Fast Fourier Transform on the bases of using new technique entitled Dynamic Random Linear Regression as allocation to hide secret message. The proposed approach is an attempt to present a transform linguistic steganography using levels for hiding to improve implementation of kashida, and improve the security of the secret message by using Dynamic Random Linear Regression.

Are testing this method in terms of security and capacity, transparency, and robustness and this is way better than previous methods. The proposed algorithm optimized steganography properties.

***Keywords:*** Arabic script, Linguistic Steganography, Dynamic Random Linear

*Regression, Kashida, Transform Based*

**إخفاء المعلومات لنصوص اللغة العربية بالاعتماد على  
الديناميكية العشوائية للانحدار الخطي**

أ.م.د. هناء محسن احمد      ميساء عبدعلي خضر  
قسم علوم الحاسوب / الجامعة التكنولوجية - العراق ابغداد

**الملخص:**

في هذا البحث لدينا معالجة مشكلة كل البحوث السابقة والتي استخدمت إخفاء المعلومات داخل النصوص ويمكن الهجوم عليها بسهولة. ولكن عندما استخدمت طريقة الإخفاء باستخدام الكاشيدة أو الغاء الكاشيدة بغية منع الهجوم في هذه الطريقة. في هذا البحث قدمت طريقة جديدة وباستخدام مستويين للإخفاء، المستوى الأول هو إخفاء بواسطة تضمين والإضافة ولكن المستوى الثاني هو إخفاء بواسطة الحقن. في المستوى الأول تضمين الرسالة السرية بت واحدة في LSB في FFT وإضافة كاشيدة واحدة. واستخدام DRLR وهي NRG لإيجاد مواقع الإخفاء داخل النص. المستوى الثاني هو حقن كاشيدة واحدة أو اثنين عشوائية داخل النص.

إخفاء المعلومات اللغوي تغطي جميع التقنيات التي تتعامل مع استخدام لغة مكتوبة الطبيعية لإخفاء رسالة سرية. في هذا البحث يقدم إخفاء المعلومات اللغوي للنصوص المكتوبة باللغة العربية، وذلك باستخدام كاشيدة وتحويل فوربييه السريع على أسس باستخدام تقنية جديدة بعنوان الديناميكية العشوائية للانحدار الخطي عن تخصيص لإخفاء رسالة سرية. النهج المقترح هو محاولة لتقديم تحويل إخفاء المعلومات اللغوي باستخدام مستويات لإخفاء لتحسين تنفيذ كاشيدة، وتحسين أمن الرسالة السرية باستخدام العشوائية الديناميكية الانحدار الخطي.

تم اختبار هذه الطريقة من الناحية الأمنية والقدرات، والشفافية، ومثانة، وهذا هو وسيلة أفضل من الطرق السابقة. الخوارزمية المقترحة الأمثل خصائص إخفاء المعلومات.

## **1- INTRODUCTION**

Linguistic steganography is focused on apply changes to a cover text so as to embed secret message, in a way that the changes do not caused any unnatural or ungrammatical text. According to cover text, linguistic steganography can be classified into two categories: generation based such as in [1], or transformation based such as in [2]. Linguistic steganography, as depicted in Figure (1), is one of steganography main branches, beside Technical steganography, and Digital steganography [3], [4]. Which consists of two types:

1. Semagrams: This hides information by using of sign or symbols. There are two types of semagrams: Visual semagrams: the visual semagrams uses

ordinary physical objects , above suspicion viewing to carry a message for example doodles , components positioning on website , desk [3], and Text Semagrams: the text semagrams hides a message by modifying the carrier text appearance for example subtle alteration in font type or size, extra space addition , varied trappings in hand written text , letters [3].

2. Open codes: hide a secret message with a legitimate carrier message in such a ways that are obvious to an unsuspecting. There are two types of Open code: Jargon code: this uses languages that is understood by a group of people but is meaningless to other people, and Covered Ciphers: "described that covered or concealment ciphers hides a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed". There are two types of covered ciphers: "Grill ciphers: employs a template that is used to cover the carrier message and the words that exist in the template openings are the hidden message, and Null Ciphers: According to some prearranged set of norms null cipher hid the message such as read every 5<sup>th</sup> word or view at the 3rd character in each word" [3].

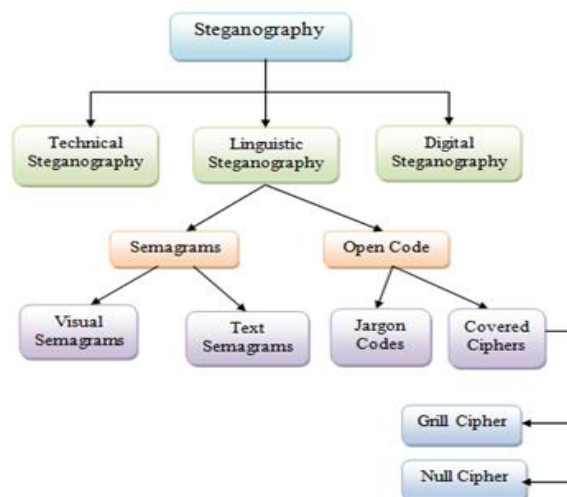


Figure (1): Type of Linguistic Steganography [3].

In our present, we proposed layers steganography technique for script written in Arabic language using Fast Fourier Transform (FFT) and kashida. The proposed approach use Dynamic Random Linear Regression (DRLR) as generate random location, to embed the secret message bits using FFT and kashida as a first layer followed by add kashida characters randomly as second layer. The proposed algorithm optimized steganography properties such as transparency, robustness, and security of the secret message for Arabic script based secure communication.

The other sections of the paper are structured as: Section II presents the literature review for kashida based linguistics steganography and explain fundamental used of proposed system. Section III explain algorithm for

proposed system and results and discussions are done in section V, and IV deals with the conclusion.

## 2- LITERATURE REVIEW AND FUNDAMENTAL USED IN PROPOSED SYSTEM

### A. Literature review

Kashida is an Arabic redundant character which is used to justify the text, without affect the meaning of words. The Researchers suggested using one kashida as bit zero, and two kashida as bit one, or vice versa.

In 2007, A. Gutub, and M.Fattani, introduced a novel Arabic text steganography technique for Arabic script using letter points and kashida. The technique hides secret information as bits in Arabic letters (cover) by using kashida and points of letters. The technique consider un-point Arabic letters followed by a kashida if the secret bit is (0), and pint Arabic letters followed by kashida if secret bit is (1).

Their technique enhanced robustness and security but might have some limitation with capacity of the cover media if the number of secret bits of the secret information is large. This steganography technique is found to be suitable for other languages having similar scrip to Arabic for example Persian and Urdu [5].

In 2009, A. H. Fahd, G. Adnan, A. K. Khalid, and H. Jameel, Introduced improving security, and capacity for Arabic text steganography using Kashida. The approach hides secret information as bits within Arabic letters (cover) by using kashida using three scenarios. The approach discussed maximum number of Kashida letters that can be added to the Arabic cover word. Also the researchers evaluated the number of hidden bits that can be embedded in the carrier file and compared the results with diacritics, and Kashida methods [6]

In 2010, Adnan Abdul-Aziz Gutub, Wael Al-Alwani, and Abdulelah BinMahfoodh, introduced an improved Arabic text steganography technique for Arabic script using kashida. The approach hides secret information as bits within Arabic letters (cover) by using extension character (kashida). The technique considers one kashida if the secret bit is (0) and two kashida if secret bit is (1) after any letter can hold it. The finishing character is embedding just after the last bit of the secret information, then the kashida as is embed randomly to the rest script in order to enhance the security of the technique. Also their technique enhanced security, capacity and robustness for Arabic scripts based secure communication [7].A. Ali and F. Moayad, Introduced Arabic text steganography technique for Arabic script using kashida with Huffman code. The approach hides secret information as bits within Arabic letters (cover) by using extension character (kashida), and compressed the stego file using Huffman code. The technique considers absence of kashida if the

secret bit is (0) and one kashida if secret bit is (1) after any connected letters. Also their technique applied to other than Arabic script based secure communication, with different document formats [8].

In 2013, Ammar Oden, Khaled Elleithy, Miad Faezipour, introduced an improved Arabic text steganography technique for Arabic script using variation kashida. The approach pick one of four scenarios randomly to hides secret information as bits within Arabic letters (cover) by using kashida. The technique considers un-point Arabic letters followed by a kashida if the secret bit is (0), and point Arabic letters followed by kashida if secret bit is (1) as first scenario , and vice versa as second senior. The third senior is adding kashida after Arabic letters if the secret bit is (1) and (0) otherwise, vice versa as forth senior. Also their technique enhanced security, complexity for Arabic script based secure communication [9].

### B. Fast Fourier Transform and its Inverse

The mathematical formula to Fourier Transform of a time domain function  $f(x)$ , for real numbers  $x$  and  $y$  is [10]:

$$F(y) = \int_{-\infty}^{+\infty} f(x) \exp[-i2\pi xy] dx \quad \dots\dots\dots (1)$$

And the mathematical formula to its inverse is [10]:

$$f(x) = \int_{-\infty}^{+\infty} F(y) \exp[i2\pi xy] dy \quad \dots\dots\dots (2)$$

$f(x)$  : Time domain function

$F(y)$ : Frequency domain function

$x$ : Argument with units of time

$y$ : Argument with units of frequency

$e$ : Base of natural logarithms

$i$ : Imaginary unit ( $i^2 = -1$ ).

### C. Linear Regration (LR)

Linear regression attempts to model the relationship between two variables  $X$ , and  $Y$ , by fitting a linear equation to observed data, such as [11]:

$$Y = a + b X_i \quad \dots\dots\dots(3)$$

Where

$X$  = The explanatory variable

$Y$  = The dependent variable

$b$  = The slope of the line

$a$  = The value of  $y$  when  $x = 0$ .

### D. DRLR

Is a new technique to generate a set of random positions  $X_i$

$I = 1.2\dots N$  by using this equation

$$X_i = a + bX_{i-1} \quad \dots\dots\dots(4)$$

Where

N = The size of generated random positions  
 $X_{i-1}$  = The explanatory variable  
 $X_i$  = The dependent variable  
 b = The slope of the line  
 a = The value of  $X_i$  when  $X_{i-1} = 0$ .

3- PROPOSED SYSTEM

A. Idea for proposed system

The proposed approach main idea as depicted in Figure (2) the embedding, and Figure (3) the extraction, is to use DRLR as generated random location, to added random kashida characters to the rest Arabic word scripts as a second layer, where the first layer is inject the secret message bits in the inverse FFT (LSB of (real (FFT) of selected Arabic script word))), and then apply one kashida character. The first addition of kashida is for the hiding process of the secret information, while the second addition of the kashida is for confusion purpose to insure security of the secret message.

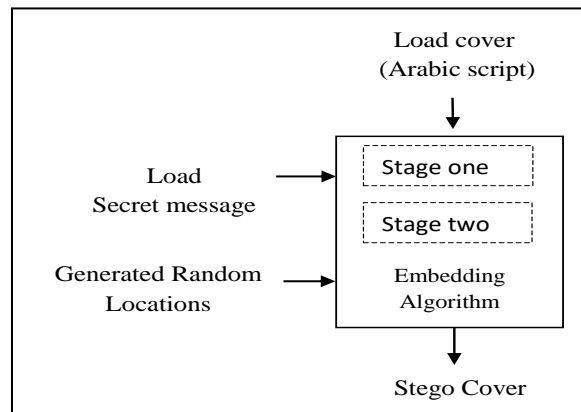


Figure (2): The proposed hiding process

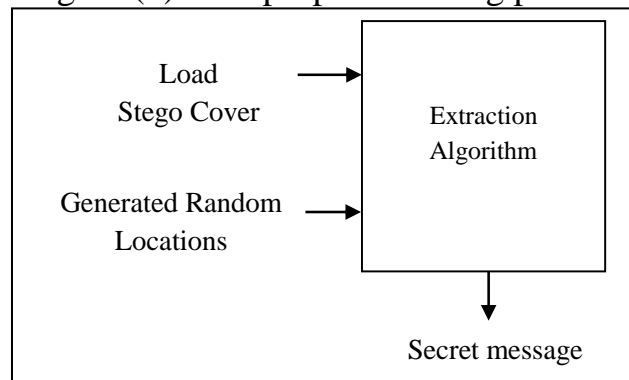


Figure (3): The proposed extraction process.

*B. Embedding process*

Embedding Algorithm:

Input: secret message, seed, a, b, N, set of Arabic scripts.

Output: stego-cover.

Process:

Step1. Secret message binarization: The secret message is hidden in form of (0) s, and (1) s, which represent (64) bit Unicode of each character using the hexadecimal representation.  $N$ , is the total number of secret message bits. Figure (4) presents the binarization process to secret message. Figure (5) is a simple example of applying binarization process to secret message.

Step2. Generate Random positions: The process of generated random positions, using DRLR, start by using secret key (seed) to generate sequence of random values  $c_i$ , where  $0 \leq c_i < 32$ . The values  $c_i$ , represents offset of Arabic script words to start the embedding process. The total number of Generate Random positions is  $(N)$ , where  $N$ , is the total number of secret message bits.

Step3. Cover selection: select Arabic script (cover) that can hold input secret message bits.

Step4. Do while not end of Arabic script words

Step5. Embedding layer one: For each secret message bit and Generate Random positions  
do

Step6. Use  $c_i$  value as offset to next word to embed the secret message bit, into inverseFFT (LSB (real (FFT (select Arabic script word))))), then apply one kashida if the secret message bit is one or if the secret message bit is zero.

Step7. End of For.

Step8. Else

Step9. Embedding layer two: add kashida characters randomly to the rest Arabic script words

Step10. End of Do.

Step11. End

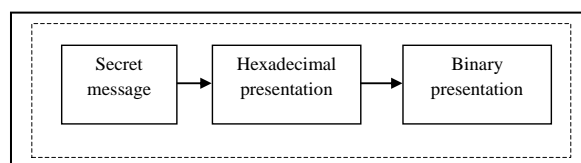


Figure (4): Secret Message Binarization.

Secret message	كم تطلبون لنا عيبا فيعجز
Hexadecimal representation	20FCEF2020AAD7FBA9E8F22020FBF2C72020D FFDA9C72020BAFDDFADD2
Binary representation	001000001111110011101111001000000010000 01010101011010111111101110101001111010 001111001000100000001000001111101111110 010110001110010000000100000110111111111 110110101001110001110010000000100000101 1101011111101110111111010110111010010

Figure (5): Secret Message Binarization Example.

**C. Extraction Process**

Extraction Algorithm:

Input: secret message, seed, a, b, N, stego cover.

Output: secret message.

Process:

- Step1. Generate Random positions: The process of generated random positions, using DRLR, start by using secret key (seed) to generate sequence of random values  $c_i$ , where  $0 \leq c_i < 63$ . The values  $c_i$ , represents offset of Arabic script words (stego-cover) to start the extraction process.
  - Step2. Loading: Load stego-cover, and Generate Random positions.
  - Step3. For each Generate Random Positions do
  - Step4. Use  $c_i$  value as offset to next word to extract the secret message bit, from LSB of select Arabic script word (stego-cover).
  - Step5. End of For.
  - Step6. Converts each seven bits into one letter the result is the secret message.
- End.

**4- RESULTS AND DISCUSSION**

In this section we discuss to cases to ensure the proposed technique security:

Case one: An example result for applying the proposed technique using embedding

layer one, as depicted in Figure (6).



Cover	<p>معلوم كما يجلب عن الملام ووقع فعاله فوق الكلام ذراني والقلاة بلا دليل ووجهي والهجير بلا لثام  فاني أستريح بندي وهذا وأتعب بالإناخة والمقام عيون رواجلي إن حرت عيني وكل بعام رازحة  بغامي فقد أرد المياه بغير هاد سوى عدي لها برق الغمام بدم لمهجتني ربي وسيفي إذا احتاج  الوحيد إلى النمام ولا أمسى لأهل البخل ضيقا وليس قرى سوى مخ النعام ولما صار ود الناس  خبا جزيت على ابتسام بابتسام وصرت أشك فيمن أصطفيه لعلمي أنه بعض الأنام ما في المقام  لذي عقل وذو أدب من راحة فدع الأوطان واعترب سافر تجد عوضا عن تفارقه وانصب</p>
Secret message	<p>كم تطلبون لنا عيبا فيعجز</p>
Stego-cover	<p>معلوم كما يجلب عن الملام ووقع فعاله فوق الكلام ذراني والقلاة بلا دليل ووجهي والهجير  بلا لثام فاني أستريح بندي وهذا وأتعب بالإناخة والمقام عيون رواجلي إن حرت عيني  وكل بعام رازحة بغامي فقد أرد المياه بغير هاد سوى عدي لها برق الغمام بدم  لمهجتني ربي وسيفي إذا احتاج الوحيد إلى النمام ولا أمسى لأهل البخل ضيقا  وليس قرى سوى مخ النعام ولما صار ود الناس خبا جزيت على ابتسام بابتسام وصرت  أشك فيمن أصطفيه لعلمي أنه بعض الأنام ما في المقام لذي عقل وذو أدب من راحة فدع  الأوطان واعترب سافر تجد عوضا عن تفارقه وانصب</p>

Figure (6): Proposed Technique example of embedding layer one.

We can conclude from case one that is visually easy to find the locations of secret message that is embed in stego-cover.

**Case two:** An example for applying the proposed technique using embedding layer one and applying the proposed technique (embedding layer one and layer two) as depict in Figure (7-a, b) using the same secret message. This case given high level in information hiding security.

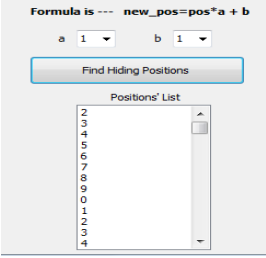
Cover	<p>لقد أخضع المتنبي مهارته الأسلوبية لإبتارته الخاصة فهو شاعر متحرر مما يمليه المقام ولا يضبط اختياراته تبعاً لما يتطلبه الموقف ، لذلك نجده يختار الألفاظ ذات المعاني غير المألوفة و يحتملها في شعره مع إمكان استبدالها بغيرها على أن طبيعة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا ينظر الممدوح فقط لأن صورة المتلقي تتراءى أمامه ولا تغيب عنه فالمتلقي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر العمل الإبداعي الشعري وأحد مؤومات جودته وقد</p>
Secret Message	<p>على قدر اهل العزم تأتي العزائم</p>
RGN DRLR	
Stego-Fourier	<p>من أساليب لإبتارته الخاصة فهو شاعر متحرر لقد أخضع المتنبي مهارته ب يمليه المقام ولا يضبط اختياراته تبعاً لما يتطلبه الموقف ، لذلك نجده يختار الألفاظ ذات المعاني غير المألوفة و يحتملها في شعره مع إمكان استبدالها بغيرها على أن طبيعة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا ينظر الممدوح فقط لأن صورة المتلقي تتراءى أمامه ولا تغيب عنه فالمتلقي هو الغائب الحاضر الصورة إن أوم عناصر العمل الإبداعي الشعري صورة من الغائب الحاضر الصورة إن ا نقاد عناية خاصة سواء تعلقوا بأحد مقومات جودته وقد أولى لها الدارزون وا شعر وبقده بوصفها الأمر بالذئمي أو المحدثين وتعد معياراً قنياً في دراسة ا اختيار الأديق وقعا على نفسية آف القيمة جمالية تحددتها أخبلة الشعراء وبراعته متلقيهم لأنها تمثل وقياس تعلمه اعقولنا على الذي نراه بأبصارنا فضلاً عن كونها وسيلة لنقل فكرة الأديب وتطبيقاته وهي تستوعب أبعاد الخيال المدرك</p>
Stego-cover using first layer	<p>لقد أخضع المتنبي مهارته الأسلوبية لإبتارته الخاصة فهو شاعر متحرر مما يمليه المقام ولا يضبط اختياراته تبعاً لما يتطلبه الموقف ، لذلك نجده يختار الألفاظ ذات المعاني غير المألوفة و يحتملها في شعره مع إمكان استبدالها بغيرها على أن طبيعة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا ينظر الممدوح فقط لأن صورة المتلقي تتراءى أمامه ولا تغيب عنه فالمتلقي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر</p>
Stego-cover using Second layer proposed technique	<p>لقد أخضع المتنبي مهارته الأسلوبية لإبتارته الخاصة فهو شاعر متحرر مما يمليه المقام ولا يضبط اختياراته تبعاً لما يتطلبه الموقف ، لذلك نجده يختار الألفاظ ذات المعاني غير المألوفة و يحتملها في شعره مع إمكان استبدالها بغيرها على أن طبيعة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا ينظر الممدوح فقط لأن صورة المتلقي تتراءى أمامه ولا تغيب عنه فالمتلقي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر</p>

Figure (7-a): Proposed technique example of embedding

Cover	في العصر العباسي وفي أوائل القرن الرابع الهجري وفي العاشر الميلادي وفي حي من أحياء الكوفة ولدت شخصية هامة وبارزة شخصية استطاعت أن تبرز نفسها بشجاعته وقوة شخصها ألا وهي شخصية أبي الطيب المتنبي شاعر كل العصور الشاعر الذي استطاع أن يعبر بشعره عن مطامح الإنسان العربي عن مآسبه ووجدانياته وآماله وتطلعاته والمنتني كما قال عنه النقاد والباحثون في بستان الحب تجده شجرة رمان كما تجده في ساحة الحرب شجرة سيوف والمنتني خلاصة الثقافة العربية الإسلامية في النصف الأول من القرن الرابع للهجرة هذه الفترة كانت فترة نضج حضاري
Secret Message	القمر انو لله سر في علاك
RGN DRLR	
Stego-Fourier	القرن الرابع الهجري وفي العاشرة في العصر العباسي وفي أوائل حي من أحياء الكوفة ولدت شخصية هامة وبارزة شخصية الميلادي وفي استطاعت أن تبرز نفسها بشجاعته وقوة شخصها ألا وهي !شخصي أبي الطيب المتنبي شاعر كل العصور الشاعر الذي استطاع أن يعبر بشعره عن مطامح الإنسان العربي عن مآسبه ووجدانياته وآماله وتطلعاته والمنتني كما قال عنه النقاد والباحثون في بستان الحب تجده شجرة رمان كما تجده في ساحة تجذب سجرة سيوف والمنتني!خلاصة الثقافة العربية الإسلامية في النصف الأول من الغرة ثلرابع للهجرة هذه الفترة كانت فترة نضج حضري في تصدع سياسي وتوتر وصراع العصر العباسي وهي في الوقت نفسه كانت فترة عاشها العالم العربي . فالخلاقة في بغداد انتحسرت هبتها والسلطان الغلي في أيدي الوزراء وقادة الجيوش ومعظمهم من الأعاجم ثم ظهور الدويلان
Stego-cover using first layer	في العصر العباسي وفي أوائل القرن الرابع الهجري وفي العاشر الميلادي وفي حي من أحياء الكوفة ولدت شخصية هامة وبارزة شخصية استطاعت أن تبرز نفسها بشجاعته وقوة شخصها ألا وهي شخصية أبي الطيب المتنبي شاعر كل العصور الشاعر الذي استطاع أن يعبر بشعره عن مطامح الإنسان العربي عن مآسبه ووجدانياته وآماله وتطلعاته والمنتني كما قال عنه النقاد
Stego-cover using Second layer proposed technique	في العصر العباسي وفي أوائل القرن الرابع الهجري وفي العاشر الميلادي وفي حي من أحياء الكوفة ولدت شخصية هامة وبارزة شخصية استطاعت أن تبرز نفسها بشجاعته وقوة شخصها ألا وهي شخصية أبي الطيب المتنبي شاعر كل العصور الشاعر الذي استطاع أن يعبر بشعره عن مطامح الإنسان العربي عن مآسبه ووجدانياته وآماله وتطلعاته والمنتني كما قال عنه النقاد

Figure (7-b): Proposed technique example two of embedding

We can conclude from case two that is visually not easy to find the locations of secret message that is embed in stego-cover.

**Case three:** An example result for applying the proposed technique using embedding

layer one the Steganography have no change, this state indicates to robustness. As depicted in figure (8).

Stego-cover scanner .PDF	لقد أخضع المتنبّي مهارته الأسلوبية لإشاراتّه الخاصّة فهو شاعر متحرر مما يملّيه المقام ولا يضبط اختياراته تبعاً لما يتطلّبه الموقف ، لذلك تجده يختار الألفاظ ذات المعاني غير المألوفة و يقحمها في شعره مع إمكان استبدالها بغيرها على أن طبيعّة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا يتنظر الممدوح فقط لأن صورة المتلقّي تتراءى أمامه ولا تغيب عنه فالمتلقّي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر العمل الإبداعي الشعري وأحد مقومات جودته وقد أولى لها الدارسون والتقدّ عناية خاصّة سواء تعلّق الأمر بالسفداسي
Stego-cover .DOCX Layer one	لقد أخضع المتنبّي مهارته الأسلوبية لإشاراتّه الخاصّة فهو شاعر متحرر مما يملّيه المقام ولا يضبط اختياراته تبعاً لما يتطلّبه الموقف ، لذلك تجده يختار الألفاظ ذات المعاني غير المألوفة و يقحمها في شعره مع إمكان استبدالها بغيرها على أن طبيعّة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا يتنظر الممدوح فقط لأن صورة المتلقّي تتراءى أمامه ولا تغيب عنه فالمتلقّي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر العمل الإبداعي الشعري وأحد مقومات جودته وقد أولى لها الدارسون والتقدّ عناية خاصّة سواء تعلّق الأمر بالسفداسي

Figure (8): Proposed technique example robustness in layer one.

**Case four :** An example result for applying the proposed technique using embedding layer two the steganography have no change, this state indicates to robustness. As depicted in figure (9).

Stego-cover scanner .PDF Layer two	لقد أخضع المتنبّي مهارته الأسلوبية لإشاراتّه الخاصّة فهو شاعر متحرر مما يملّيه المقام ولا يضبط اختياراته تبعاً لما يتطلّبه الموقف ، لذلك تجده يختار الألفاظ ذات المعاني غير المألوفة و يقحمها في شعره مع إمكان استبدالها بغيرها على أن طبيعّة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا يتنظر الممدوح فقط لأن صورة المتلقّي تتراءى أمامه ولا تغيب عنه فالمتلقّي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر العمل الإبداعي الشعري وأحد مقومات جودته وقد أولى لها الدارسون والتقدّ عناية خاصّة سواء تعلّق الأمر بالسفداسي أو المحدثين
Stego-cover .DOCX Layer two	لقد أخضع المتنبّي مهارته الأسلوبية لإشاراتّه الخاصّة فهو شاعر متحرر مما يملّيه المقام ولا يضبط اختياراته تبعاً لما يتطلّبه الموقف ، لذلك تجده يختار الألفاظ ذات المعاني غير المألوفة و يقحمها في شعره مع إمكان استبدالها بغيرها على أن طبيعّة الشاعر ونفسيته وراء اختيار هذا النوع من الألفاظ فهو لا يتنظر الممدوح فقط لأن صورة المتلقّي تتراءى أمامه ولا تغيب عنه فالمتلقّي هو الغائب الحاضر الصورة إن الصورة من أهم عناصر العمل الإبداعي الشعري وأحد مقومات جودته وقد أولى لها الدارسون والتقدّ عناية خاصّة سواء تعلّق الأمر بالسفداسي أو المحدثين

Figure (9): Proposed technique example robustness in layer one.

**Case five:** In this proposed technique, when delete all kashida retain hide information.

Because the hide a secret message in FFT in LSB and transform the FFT to

IFFT in layer one. The attack not known on detected a secret message. This Technique is given high security. After apply Jaro-Winkler method, as depicted in table (1), table (2), and table (3).

- The Jaro-Winkler method is distance measures the similarity between two strings.

The Jaro distance is: 
$$dj = \frac{1}{3} \left( \frac{m}{|s1|} + \frac{m}{|s2|} + \frac{m-t}{m} \right)$$

$t = \max\{[|S1|, |S2|]/2\} - 1$ . Explain in table (1) below:

If the word is شخصية without stego,  $dj = 1/3(5/5 + 5/5 + 5-1/5) = 0.9333$

where  $t = 1$

If the word is شخصية stego in layer one,  $dj = 1/3(6/6 + 6/6 + 6-1/6) = 0.9444$

Where  $t=2$

else the word is شخصية stego in layer two,  $dj = 1/3(7/7 + 7/7 + 7-2/7) = 0.9047$

cover without stego

	ش	خ	ص	ي	ة
ش	1	0	0	0	0
خ	0	1	0	0	0
ص	0	0	1	0	0
-	0	0	0	0	0
ي	0	0	0	1	0
ة	0	0	0	0	1

Stego cover  
Layer one

Table (1): similarity between cover and stego cover in layer one.

cover without stego

	ش	خ	ص	ي	ة
ش	1	0	0	0	0
خ	0	1	0	0	0
ص	0	0	1	0	0
-	0	0	0	0	0
-	0	0	0	0	0
ي	0	0	0	1	0
ة	0	0	0	0	1

Stego cover  
Layer two

Table (2): similarity between cover and stego cover in layer two.

No of cover	Secret message size (Byte)	Secret message size (KB)	Carrier file size (Byte)	Carrier file size (KB)	Average of hide capacity ratio %
1	11264	11	15360	15	0.7333 B or KB
2	11264	11	23552	23	0.4782 B or KB

Table (3): Explain hide capacity ratio in proposal algorithm.

**Case six:** In this proposed technique is very high transparency, because not seen in hu-

man vision and not clear for attack. Especial when the text without kashida

and one or two kashida . As depicted in figure (10).

cover	بدأ المتنبي حياته الفنية تلميذا بارعا في مدرسة أبي تمام ومضى يرسم خطاه ويفتني أثره في خطواته الأولى على الطريق الفني الذي كان أبو تمام يضرب بخطاه الثابتة القوية فيه متبيرا من حوله تلك الضجة النقدية الضخمة التي شغلت القرن الثالث ووضعت على قمة حركة التجديد فيه ممثلا لتلك المدرسة الجديدة التي شق دروبها الأولى رائدها الأول مسلم
Stego-cover Layer one	بدأ المتنبي حياته الفنية تلميذا بارعا في مدرسة أبي تمام ومضى يرسم خطاه ويفتني أثره في خطواته الأولى على الطريق الفني الذي كان أبو تمام يضرب بخطاه الثابتة القوية فيه متبيرا من حوله تلك الضجة النقدية الضخمة التي شغلت القرن الثالث ووضعت على قمة حركة التجديد فيه ممثلا لتلك المدرسة الجديدة التي
Stego-cover Layer two	بدأ المتنبي حياته الفنية تلميذا بارعا في مدرسة أبي تمام ومضى يرسم خطاه ويفتني أثره في خطواته الأولى على الطريق الفني الذي كان أبو تمام يضرب بخطاه الثابتة القوية فيه متبيرا من حوله تلك الضجة النقدية الضخمة التي شغلت القرن الثالث ووضعت على قمة حركة التجديد فيه ممثلا لتلك المدرسة الجديدة التي

Figure (10): Proposed technique example Transparency in layer one and layer two

**Case seven:** In this proposed technique the capacity is change during hiding a secret

message, because in the first state is convert Arabic text to FFT and two state is addition the kashida in layer one and injection in layer two. The amount of hiding data is increase in cover, because addition and injection in file carrier imply relative increase in stego cover. The equation below is:

Hidden Ratio = amount of hidden data / carrier file size

For example:

Hide Ratio = 11 KB/15 KB = 0.7333

Hide Ratio = 11 KB/23 KB = 0.4782

#### 5- CONCLUSION:

In this paper a new layers Arabic language steganography is implemented using the FFT implementation and Kashida as an embed process, and DRLR as random location generator to embed the Arabic secret message in the Arabic script. We present some conclusions bellow:

1. Applying Steganography methods to document (text) files as a cover which is written by Arabic language is difficult, due to the visually sensitivity of Arabic letters to any miner change as in case one.
2. The DRLR is fast search algorithm, which is improved to use as means to allocate randomly positions in the cover media (Arabic scripts) to perform the embedding operation.
3. As embedding methods, usually frequency method is harder against attack than time domain method, so using FFT and Kashida as embedding method, which improve its security agents attack.

4. Algorithm robustness: The proposed algorithm prohibits any change to carrier (Arabic script) during the transmission process since the hidden secret message does not change the cover (Arabic script) file properties such as, file size, content, and format during the transmission.
5. Algorithm transparency: the proposed algorithm improves the transparency property by hiding secret message inside the Arabic script using FFT. In addition another layer of hiding is applied using Kashida.
6. Algorithm security: the proposed algorithm improves the security property by hiding secret message inside the Arabic script using FFT and apply kashida as first layer then apply kashida as second layer to the rest Arabic script.
7. Algorithm Capacity: This algorithm is more capacity after hide a secret message in cover Arabic text as the equation is:

$$\text{Hidden Ratio} = \text{amount of hidden data} / \text{carrier file size}$$



***References***

- [1] Hana'a M. Salman, " A Natural Language Steganography Technique for Text Hiding Using LSB's", Eng.&Tech. Vol.26,No3,2008.
- [2] Xiaoxi Hu, Gang Luo, Yongjing Lu, and Lingyun Xiang,"A Steganography on Synonym Frequency Distribution", Advances in information Sciences and Service Sciences(AISS), Vol.5, no.10, May 2013.
- [3] Ching - Yun Chang, and Stephen Clark, "Adjective Deletion for Linguistic Steganography and secret sharing", Proceedings of Coling 2012: Technical Papers, pages 493–510, Mumbai, December 2012.
- [4] M. K. Kaleem,"An Overview of Various Forms of Linguistic Steganography and Their Applications Protecting Data", Journal of Global Research in Computer Science, Volume 3, No. 5, May 2012.
- [5] Adnan Abdul-Aziz Gutub, and Manal Mohammad Fattani," A Novel Arabic Text Steganography Method Using Letter Points and Extensions", International Journal of Computer, Information, Systems and Control Engineering Vol : 1 No:3, 2007.
- [6] A.-H. Fahd, G. Adnan, A.-K. Khalid, and H. Jameel, "Improving security and capacity for Arabic text steganography using 'Kashida 'extensions," presented at the IEEE/ACS International Conference on Computer Systems and Applications, 2009.
- [7] Adnan Abdul-Aziz Gutub, Wael Al-Alwani, and Abdulelah Bin Mahfoodh, "Improved Method of Arabic Text Steganography Using the Extension 'Kashida' Character", Bahria University Journal of Information &Communication Technology Vol. 3, Issue 1, December 2010.
- [8] A. Ali and F. Moayad, "Arabic text steganography using kashida extensions with Huffman code," *Journal of Applied Sciences*, vol. 10, pp. 436-439, 2010.

[9] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in Arabic text using

Kashida variation algorithm (KVA)," in Systems, Applications and Technology

Conference (LISAT), 2013 IEEE Long Island, 2013, pp. 1-6.

[10] William H. Press, Saul A. Teukolsky, William T. Vetterling, Brian P. Flannery,

Michael Metcalf," Numerical-Recipes-in-C-Second-Edition.", Cambridge

University Press; 2 edition (October 30, 1992).