

## Hiding digital image watermarking in a sound signal using Wavelet Transform and Singular Value Decomposition

Alyaa Moufaq Abdul Majeed Haleem

AIAA Zakaria

AlyaaHaleem@uomosul.edu.iq

College of Computers Sciences and Mathematics

University of Mosul, Mosul, Iraq

Received on: 04/09/2009

Accepted on: 16/05/2010

### ABSTRACT

The outgrowing of multimedia applications in communications network brought about an increasing need to provide qualified methods to protect these media and secure communication. These methods include encryption and information hiding.

In this research, a new method has been improved to hide watermarking image in voice signal then send it through the network with no effect on the cover sound through the hiding process. This method is performed by applying two ways. The first one is the discrete wavelet transform (DWT) while the second one is singular value decomposition (SVD) by using wavelet transform, we get detail values which are arranged in a specific way and then entered to the singular value decomposition algorithm. Finally we get eign values, which embedding the data of the watermark image inside these values. So, we get the watermark signal with no effects. Also, the recovered image efficiency measurement is performed by using the correlation coefficient between the original and the recovered watermark image and also we apply the measurement of the difference between the original voice signal (cover) and the watermarked voiced signal by using signal to noise ratio (SNR). Matlab is the approval as a programming language in this paper.

**Keywords:** SVD, information Hiding, watermark, eign value.

إخفاء العلامة المائية داخل إشارة الصوت باستخدام التحويل المويجي وتقنية تحليل القيمة المفردة

الأء زكريا محمد

علياء موفق عبد المجيد

كلية علوم الحاسوب والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ قبول البحث: 2012\12\04

تاريخ استلام البحث: 2012\06\26

### المخلص

أدى النمو المتزايد لتطبيقات الوسائط المتعددة على شبكات الاتصال إلى زيادة الحاجة إلى توفير طرائق كفوءة تتضمن حماية هذه الوسائط إضافة إلى أمانية الاتصالات ومن هذه الطرائق إضافة إلى التشفير إخفاء المعلومات.

في هذا البحث تم تطوير طريقة جديدة لإخفاء صورة العلامة المائية في إشارة الصوت ثم إرسالها عبر الشبكة بدون التأثير على الغطاء عند الإخفاء ويتم ذلك باستخدام تقنيتي التحويل المويجي وتحليل القيمة المفردة. باستخدام التحويل المويجي يتم الحصول على القيم التفصيلية وترتيبها بطريقة معينة و ثم يتم إدخالها إلى خوارزمية تحليل القيمة المفردة ومنه يتم الحصول على القيم غير المعتمد عليها و تضمين بيانات الصورة داخل تلك القيم و

بهذه الطريقة يتم الحصول على الإشارة الصوتية بعد عملية التضمين بدون تأثير واضح عليها. كذلك تم قياس جودة الصورة المسترجعة باستخدام معامل الارتباط بين صورة العلامة المائية الأصلية والعلامة المائية المسترجعة وكذلك قياس مقدار الاختلاف بين إشارة الصوت الأصلي (الغطاء) والإشارة الصوتية بعد تضمين العلامة المائية باستخدام مقياس SNR. تم اعتماد Matlab كلغة برمجية في هذا البحث.

**الكلمات المفتاحية:** تحليل القيمة المفردة ، إخفاء المعلومات ، العلامة المائية .

## 1. تمهيد

أدى النمو المتزايد لتطبيقات الوسائط المتعددة على شبكات الاتصال إلى زيادة الحاجة إلى توفير طرائق كفوءة تعمل على حماية البيانات والملكية الخاصة للفرد، لذلك كان لابد من ظهور وسائل تعمل على توفير أمن لهذه الوسائط لحمايتها من التحريف، السرقة أو نشر المعلومات الحساسة منها. ومن هنا ظهرت الحاجة إلى توفير وسائل أمنية للبيانات، ومن هذه الوسائل علم التشفير Cryptography الذي يعنى بتوفير حماية لحزن البيانات ونقلها عن طريق استخدام مفتاح سري، لذلك كان التشفير وما يزال الطريقة الناجحة لحماية البيانات المخزونة والمرسلة عبر الشبكة، ولكن مع ازدياد شبكات التناقل وشبكة المعلومات العالمية Internet أصبح من الصعب المحافظة على هذه البيانات، ولاسيما أنها دائما في متناول الجميع عبر شبكة الانترنت في صيغة غير واضحة تبعث على الشك والاهتمام لدى المتطفل والسارق لفتح هذا التشفير أو تدمير المعلومات المرسله.

لقد فرضت العديد من القيود لمحاولة منع استخدام التشفير عبر الشبكة، ومن هذه القيود منع انسيابية أية معلومة لمصدر يستخدم التشفير في مراسلاته كما جاء في التشريع الصادر عن دائرة العدل الأمريكية الذي يعنى المقاطعة المعلوماتية، لذلك بدأت معظم الحكومات بفرض سيطرتها على التشفير ومنع المؤسسات من التعامل به. لذلك كان لابد من تطوير أمنية البيانات وإنشاء تقنيات ووسائل جديدة، ومن هنا ظهر علم إخفاء المعلومات [2][1].information Hiding

كان الإخفاء ومازال الطريقة الناجحة لحماية البيانات المخزونة والمرسلة عبر الشبكة لأنه يعطي أمنية عالية و يظهر عنصر الإخفاء دون أي تغيير. إن الغاية من إخفاء المعلومات ليست منع الآخرين من معرفة المعلومات المخفية فقط بل لإزالة الشك أصلا في وجود معلومات مخفية، لكي لا يحاول المتطفل معرفتها والعبث بها، والشئ المميز في تقنيات إخفاء المعلومات أنها تواكب التقنيات الحديثة، ويمكن استخدامها في جميع الوسائط الحاسوبية من صور، نصوص، صوت، فيديو وحزم الشبكة. [1]

تعد العلامة المائية إحدى طرق الإخفاء المتعددة إذ زادت في الفترة الأخيرة ظاهرة التوزيع والنسخ غير المخولين للإشارة الرقمية بشكل كبير بسبب قوة الحاسبة الشخصية مع كلفة قليلة ووثوقية عالية لوسائط الخزن وتعد العلامة المائية إحدى وسائل حماية الحقوق الفكرية.

## 2. تعريف الإخفاء

يعرف إخفاء المعلومات على انه تضمين بيانات سرية في أشكال مختلفة من الوسائط المتعددة الرقمية كملفات النصوص والصور والملفات الصوتية و الفيديوية. وهذا يعنى إخفاء (بيانات سرية) في معلومات أخرى ظاهرها لا يدعو إلى الشك ولا يلفت الانتباه، وتكون غير مدركة من المتطفلين والمهاجمين، ولذلك لن تكون البيانات السرية مشاعة لمستخدمي الشبكة، بل يبقى محتواها حكرا على الجهات ذات العلاقة، والتي تكون على

دراسة بكيفية استخراج هذا المحتوى. ومع النمو السريع لتقنيات الشبكات والاتصالات، فإن تقنيات الإخفاء أصبحت تستخدم بصورة واسعة لتحقيق أغراض متعددة منها حماية حقوق الطبع وتنشيط الملكية. [1]

### 3. خصائص متعارضة Conflicting Properties

ثمة خصائص يجب الأخذ بها عند تطبيق إحدى تقنيات إخفاء المعلومات، وهي:

- **القدرة على عدم الإدراك (Imperceptibility):** خاصية عدم تغيير الغطاء بصورة ملحوظة من قبل حواس الإنسان البصرية والسمعية.
- **القوة (Robustness):** وتعني مدى قوة تقنية إخفاء المعلومات أمام الهجمات عليها واكتشاف البيانات المخفية أو تدميرها وتشويشها، ومن هذه الهجمات الكبس بفقدان Lossy Compression، والتعرض للمرشحات الخطية واللاخطية وغيرها من الهجمات.
- **السعة (Capacity):** كمية البيانات المراد إخفاؤها داخل وسط مضيف لها من دون كشفها.
- **القدرة على عدم الاكتشاف (Undetected ability):** وهذه الخاصية تعني إن البيانات المخفية تكون غير قابلة للكشف من المهاجمين.

إن الخصائص السابقة تكون متعارضة فيما بينها ولا يمكن تحقيقها جميعا في وقت واحد، ومثال ذلك إن نخفي معلومات كبيرة داخل صورة، فعند ذلك لا نحقق القوة المطلوبة ويكون من السهل اكتشاف إن ثمة بيانات مخفية من المهاجمين (تعارض خاصية السعة مع القدرة على عدم الاكتشاف)، وفي الغالب إذا كانت التقنية قوية ضد الهجمات والتشويش عليها فإن كمية البيانات المخفية ستكون قليلة، وغالبا ما يجب توفير خاصية القوة في تقنيات إثبات الملكية لأن تلك التقنيات تتطلب القوة ضد الهجمات ويقابل ذلك إخفاء بيانات قليلة نسبيا (تعارض خاصية القوة مع السعة). [4]

### 4. الدراسات السابقة

حاول الباحثون إيجاد تقنيات إخفاء متطورة تواكب التطور السريع في تقنيات الإخفاء والشبكات، فمنهم من أنجز بحثا ودراسات واسعة لربط تقنيات إخفاء المعلومات مع تقنيات الذكاء الاصطناعي، وآخرون أنجزوا الاتصال السري في شبكات الحاسوب من خلال القنوات المخفية، ومن هذه البحوث:

1. في عام 2002 قدم الباحث (Chandra DVS) بحثا لإخفاء صورة داخل صورة باستخدام التحويل المويجي وتحليل القيمة المفردة عن طريق دمج SVs للصورة الأصلية مع SVs لصورة العلامة المائية باستخدام عامل تحجيم ثابت. [6]

2. في عام 2009 قدم الباحثون (Amansouri, A mahmoudi Aznavah and Ftorkamani) بحثا لإخفاء صورة العلامة المائية داخل ملف غطاء من نوع صورة باستخدام (CWT) Complex Wavelet transform وتقنية تحليل القيمة المفردة. [5]

3. في عام 2010 قدم الباحثان (Al\_Haj Ali and Mohammad Ahmad) بحثا لإخفاء صورة العلامة المائية الثنائية داخل ملف صوتي عن طريق تطبيق أربعة مستويات للتحويل المويجي على كل مقطع من مقاطع الإشارة الصوتية وإعادة ترتيب المعاملات التفصيلية داخل مصفوفة جديدة ثم تطبيق خوارزمية تحليل

القيمة المفردة على المصفوفة الناتجة لينتج ثلاث مصفوفات هي  $U, S, V$  يتم تضمين قيم البت للعلامة المائبة  $W(n)$  داخل العنصر الأول لقطر المصفوفة  $S$  حسب المعادلة الآتية:

$$SW_{11} = S_{11} \times (1 + (\alpha \times W_{(n)})) \quad \dots(1)$$

إذ أن:  $W(n)$ : تمثل مصفوفة بيانات العلامة المائبة بالنظام الثنائي.

$S_{11}$ : تمثل العنصر الأول للقطر الرئيسي داخل المصفوفة  $S$ .

$SW_{11}$ : تمثل العنصر الأول للقطر الرئيسي داخل المصفوفة  $S$  بعد تضمين قيمة بت من العلامة

المائبة، أما قيمة  $\alpha = 0.2$ .

حيث تم إخفاء صورة ثنائية (Binary image) بحجم  $4*6$ . أما في عملية الاسترجاع فيجب وجود ملف الغطاء الأصلي بالإضافة إلى الملف المضمن إذ يتم إيجاد قيمة البت للعلامة المائبة المضمنة داخل كل مقطع حسب الآتي إذا كان الناتج من حاصل قسمة  $S11_{11} / S11$  أكبر أو مساويا 1.2 فان قيمة  $w(n)$  تكون 1 وإلا تكون  $w(n)$  مساوية للصفر. [3]

## 5. التحويل المويجي Wavelet Transform

إن القصور في تمثيل الإشارة باستخدام تحويلات فورير كان السبب وراء ظهور تقنيات التحويل المويجي، إذ أن تحويل فورير يظهر الترددات التي حدثت في الإشارة دون الإشارة إلى زمن حدوثها وهذا التمثيل لا يكون كافيا لملاحظة التغيرات المهمة في الإشارات غير الثابتة، إذ انه عندما ترسم الإشارة في مجال الزمن، فان تمثيل قيمتها في ذلك المجال يمكن الحصول عليه من الإشارة نفسها ولكن هذا التمثيل ليس دائما أفضل لتمثيل لأغلب التطبيقات المتعلقة بمعالجة الإشارة ففي العديد من الحالات تكون المعلومات الأكثر بروزا مخبأة في محتوى تردد الإشارة. [7]

إن طيف التردد للإشارة أساسا هو مكونات التردد (مكونات طيفية) لتلك الإشارة، إذ تظهر لنا ما هي الترددات الموجودة فيها. وكما هو معروف فان كل من تحويل فورير وتحويل فورير السريع تعطي معلومات عن تردد الإشارة فقط، والتي تعني بأنها تخبرنا بمقدار كل تردد موجود في الإشارة ولكنها لا تخبرنا في أي وقت او متى وجدت هذه الترددات في مجال الزمن، هذه المعلومات غير مطلوبة عندما تكون الإشارة ثابتة (الإشارات الثابتة هي الإشارات ذات المعدلات الإحصائية التي لا تتغير مع الزمن)، لذا فأن تحويل فورير مفيد لهذه الإشارات. أما الإشارات غير الثابتة (الإشارات ذات المعدلات الإحصائية التي تتغير مع الزمن) يكون استخدام فورير غير ذي جدوى، لذا نحتاج إلى تحويل يعطينا تمثيل التردد والزمن معا للإشارة المطلوب تمثيلها. وهكذا فان التحويل المويجي يعد احد التحويلات المرشحة التي تزودنا بتمثيل التردد والزمن في الوقت نفسه.

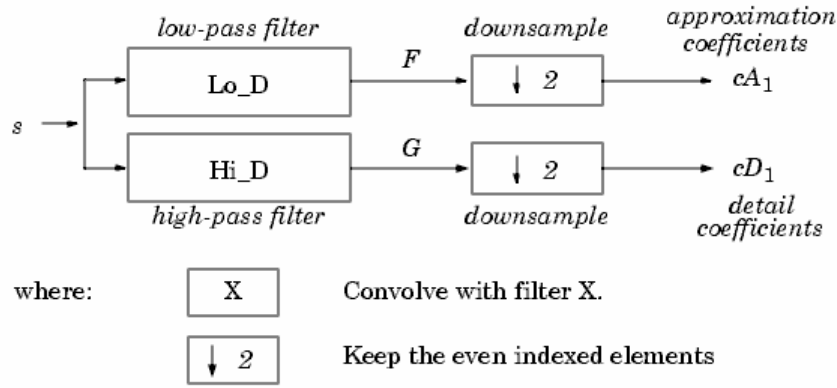
هنالك تحويلات أخرى تعطي التردد والزمن في الوقت نفسه مثل تحويل فورير ذي الوقت القصير (STFT) ولكن التحويل المويجي أكثر فائدة من STFT إذ أن STFT يعطي قرارا ثابتا في كل الأوقات، في حين أن التحويل المويجي يعطي قرارا متغيرا وحسب تفاصيل التردد والزمن معا. [7]

كما ويتميز التحويل المويجي على تحويلات فورير بميزات أخرى، فعلى سبيل المثال يعمل التحويل المويجي بشكل جيد في تقريب الإشارات ذات التغيرات الحادة أو الإشارات المنقطعة، فالتحويل المويجي يمكن أن يشكل صوت الكلام أو الموسيقى أو الفيديو وإشارات غير ثابتة أخرى. علاوة على ذلك فان التحويل المويجي يمكن أن يستعمل في العديد من التطبيقات مثل إزالة الضوضاء من الصور أو كبس الصور أو تحسين الرؤية لمشهد معين يخص الإنسان. [3]

## Discrete Wavelet Transform 1.5 التحويل الموجي المقطع

### ❖ مرحلة التحليل :

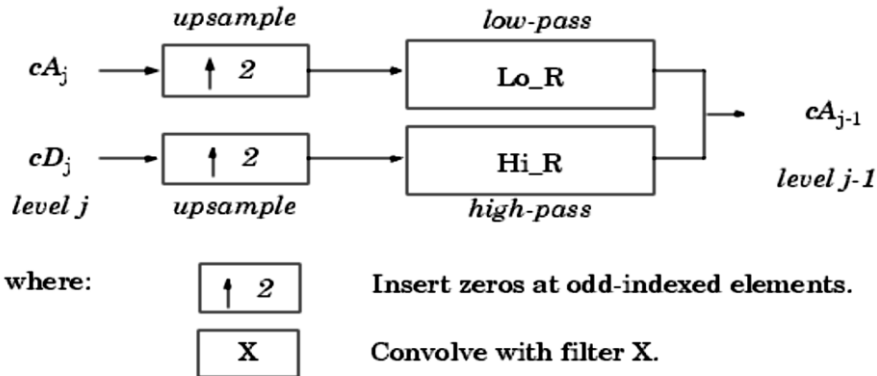
تتم عملية التحليل عن طريق إمرار الإشارة (Signal) على مرشحين الأول هو مرشح الإمرار الواسع (Low Pass Filter(Lo\_D)) أما الثاني فهو مرشح الإمرار العالي (High Pass Filter(Hi\_D)) ويتم تنفيذ عملية اللاقوف الرياضي (Convolution) وعملية التتقيص الثنائي Down sampling على إخراج المرشحين بذلك يتم الحصول على معاملات التقريب Approximation coefficients  $cA(n)$  من مرشح الإمرار الواسع (Lo\_D) والحصول على معاملات التفصيل Detail coefficients  $cD(n)$  من مرشح الإمرار العالي (Hi\_D). كما موضح في الشكل (1).



الشكل (1) يوضح مرحلة التحليل للتحويل الموجي المقطع

### ❖ مرحلة الاسترجاع:

يتم استرجاع معاملات التقريب  $cA_{j+1}(n)$  بواسطة الاستكمال أي عن طريق حشر أصفار بين كل عينتين من عينات التقريب  $cA_j(n)$  وعينات التفصيل  $cD_j(n)$  أيضا ومن ثم إدخالها إلى مرشحات الاسترجاع (Lo\_R) (Hi\_R) على التوالي لإجراء عملية اللاقوف الرياضي للحصول على الإشارة المدخلة [7]. كما موضح في الشكل (2).



الشكل (2) يوضح مرحلة الاسترجاع للتحويل الموجي المقطع

حيث نلاحظ أن التحويل الموجي المقطع لا يحتوي على عمليات تكامل أو عمليات اشتقاق وإنما تحتوي على عمليات ضرب وجمع فقط مما جعله مناسباً للاستخدام على الحاسبات الرقمية. [3]

## 6. تحليل القيمة المفردة (SVD) Single Value Decomposition

إن تقنية (SVD) مبنية على نظريات الجبر الخطي والتي تتضمن تقسيم المصفوفة المستطيلة  $A$  إلى ثلاث مصفوفات، المصفوفة المتعامدة ( $U$ ) وهي المصفوفة التي يكون حاصل ضربها في المدور لها هو مصفوفة قطرية جميع عناصر القطر لها 1 ، المصفوفة القطرية ( $S$ ) هي المصفوفة التي تكون جميع عناصرها أصفارا ماعدا عناصر القطر والمصفوفة المتعامدة ( $V$ ) هي المصفوفة التي يكون حاصل ضربها في المدور لها هو مصفوفة قطرية جميع عناصر القطر لها 1.

$$A_{mn} = U_{mn} S_{mn} V^T_{mn} \quad \dots(2)$$

حيث أن الأعمدة للمصفوفة  $u$  والتي تمثل القيم الذاتية للمصفوفة  $A A^T$  هي Orthonormal ( يطلق على المتجه الذي يكون طوله وحدة طول وحاصل ضربه مع كل vector ضمن المصفوفة يساوي صفرًا Orthonormal) وتسمى المصفوفة في ذلك الحين مصفوفة متعامدة والأعمدة للمصفوفة  $v$  هي Orthonormal القيم الذاتية للمصفوفة  $A^T A$  . وان  $S$  هي مصفوفة قطرية تحتوي الجذر التربيعي للقيم الذاتية غير الصفرية من المصفوفة  $V$  أو  $U$ . [8].

$$\begin{bmatrix} V_{1,1} & \cdot & \cdot & V_{1,n} \\ V_{2,1} & \cdot & \cdot & V_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ V_{n,1} & \cdot & \cdot & V_{n,n} \end{bmatrix} \begin{bmatrix} S_{1,1} & 0 & 0 & 0 \\ 0 & S_{2,2} & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & S_{n,n} \end{bmatrix} \begin{bmatrix} U_{1,1} & \cdot & \cdot & U_{1,n} \\ U_{2,1} & \cdot & \cdot & U_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ U_{n,1} & \cdot & \cdot & U_{n,n} \end{bmatrix}$$

## 7. الطريقة المطورة

في هذه الطريقة يتم استخدام التحويل الموجي وتحليل القيمة المفردة إذ يتم الإخفاء باستخدام المصفوفة  $V$  الناتجة بعد تطبيق تحليل القيمة المفردة وكذلك تتميز هذه الطريقة باسترجاع العلامة المائبة دون الحاجة إلى ملف الغطاء الأصلي. وتتخلص هذه الخوارزمية بالخطوات الآتية:

### 1.7 خوارزمية الإخفاء

**المدخلات:** ملف الغطاء (ملف صوتي)، صورة العلامة المائبة المراد إخفاؤها (أي صورة ملونة أو رمادية من نوع BMP أو JPG).

**المخرجات:** الملف الصوتي بعد إخفاء المعلومات.

**الخطوة الأولى:** إدخال اسم ملف الغطاء، ثم قراءة محتويات الملف وخرن العينات الصوتية في مصفوفة  $x$ .

**الخطوة الثانية:** إدخال اسم ملف العلامة المائبة، ثم قراءة محتويات الملف وخرننها في مصفوفة  $a$ .

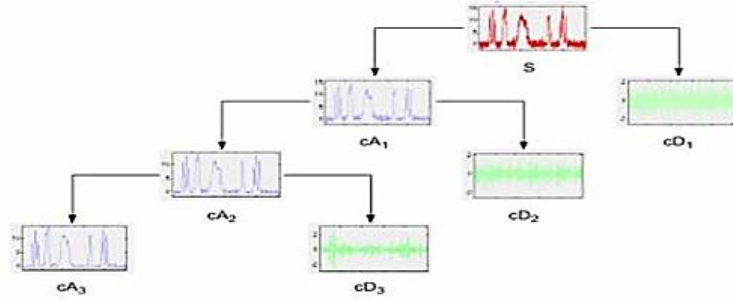
**الخطوة الثالثة:** تقسيم الإشارة الصوتية  $x$  إلى مجموعة من القوالب (Frame) حيث كل قالب بحجم 512 عينة.

**الخطوة الرابعة:** إجراء عملية تغير لأبعاد الصورة  $a$  بحيث تلائم حجم الملف الصوتي الذي تم اختياره لإخفاء الصورة بالاعتماد على الصيغة التالية

$$\frac{\text{الطول/العرض للصورة} = (\text{عدد القوالب} * 2) \text{ عدد البت المضمنة في كل قالب}}{\text{عدد البت المستخدمة في تمثيل القيم للصورة}}$$

**الخطوة الخامسة:** تحويل مصفوفة الصورة للعلامة المائية  $a$  إلى مصفوفة ذات بعد واحد ومن ثم تحويل القيم اللونية إلى النظام الثنائي ومن ثم تحويل المصفوفة الأخيرة إلى مصفوفة ذات بعد واحد أطلق عليها مصفوفة العلامة المائية  $W(n)$ .

**الخطوة السادسة:** تنفيذ أربعة مستويات للتحويل المويجي على كل قالب لينتج لدينا  $cD_1, cD_2, cD_3, cD_4$  ويمثلون مصفوفات المعاملات التفصيلية لكل مستوى وكذلك ينتج  $cA$  وهي مصفوفة المعاملات التقريبية [3]، كما موضح في الشكل (3).



الشكل (3) يوضح نتائج التحليل المويجي لقالب من الإشارة لثلاثة مستويات

**الخطوة السابعة:** ترتيب مصفوفات المعلومات التفصيلية الناتجة من الخطوة السابقة بالطريقة التالية حيث أطلق على المصفوفة الناتجة  $DC$ . حجم هذه المصفوفة هو  $4 \times x (L/2)$  ، حيث أن  $L$  يمثل حجم القالب. كما موضح في الشكل (4)

cD <sub>1</sub>							
cD <sub>2</sub>				cD <sub>2</sub>			
cD <sub>3</sub>		cD <sub>3</sub>		cD <sub>3</sub>		cD <sub>3</sub>	
cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>	cD <sub>4</sub>

الشكل (4) يوضح ترتيب مصفوفة DC

**الخطوة الثامنة:** تنفيذ SVD على مصفوفة  $DC$  ، سوف ينتج لدينا ثلاث مصفوفات هي  $U, S, V$  [3].

**الخطوة التاسعة:** تضمين الخلية الثنائية للعلامة المائية  $W(n)$  باستخدام مصفوفة  $V$ . حسب الأسلوب التالي:

- تحديد المعامل  $V(i,j)$  لتضمين قيمة بت واحد بداخله حيث يتم إيجاد معكوس القيمة  $y = 1/V(i,j)$
- تضمين بت من العلامة المائية داخل الجزء الصحيح للعدد  $y$  الناتج من القسمة بعد تحويله إلى الصيغة الثنائية إذ يتم استبدال  $W_i$  مع قيمة البت الثامن للعدد  $y$  (إخفاء داخل الخلية الثنائية الأعلى أهمية).
- إيجاد المعكوس لكل  $y$  للحصول على قيم المصفوفة  $V$  بعد التضمين حيث يشار لها  $V_w$ .

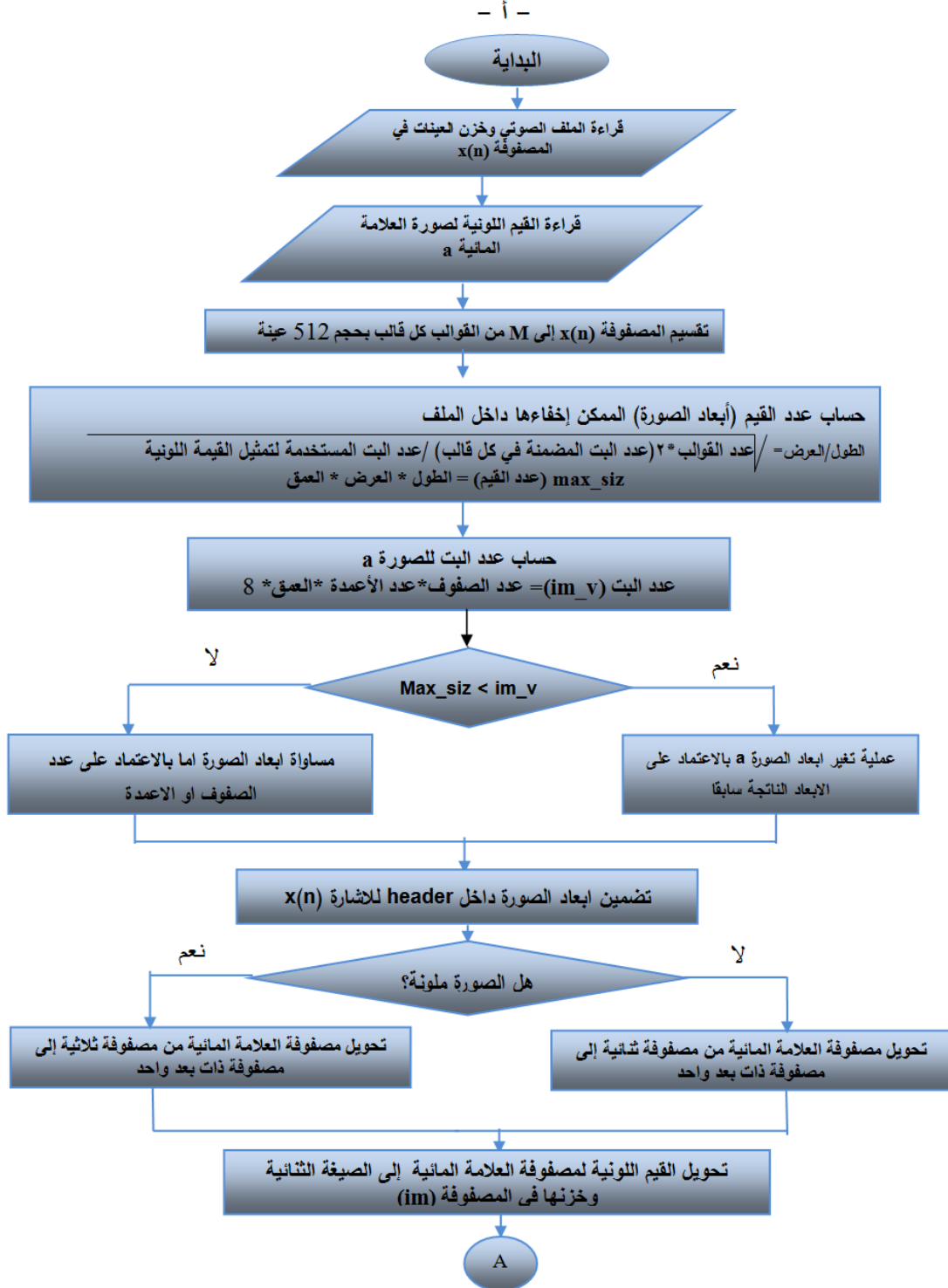
**الخطوة العاشرة:** توليد الإشارة الصوتية بعد عملية التضمين لكل البت للعلامة المائية داخلها عن طريق :

- تطبيق معكوس تحليل القيمة المفردة للحصول على مصفوفة  $DC_w$  الناتجة من عملية التضمين.
- $$DC_w = U \times S \times V_w^T \quad \dots(3)$$

• تنفيذ أربع مستويات من التحويل المويجي المعكوس على مصفوفة  $DC_w$  للحصول على القالب بعد

التضمين وأخيرا تجميع القوالب للحصول على العينات الصوتية بعد تضمين العلامة المائية  $X_w$ .

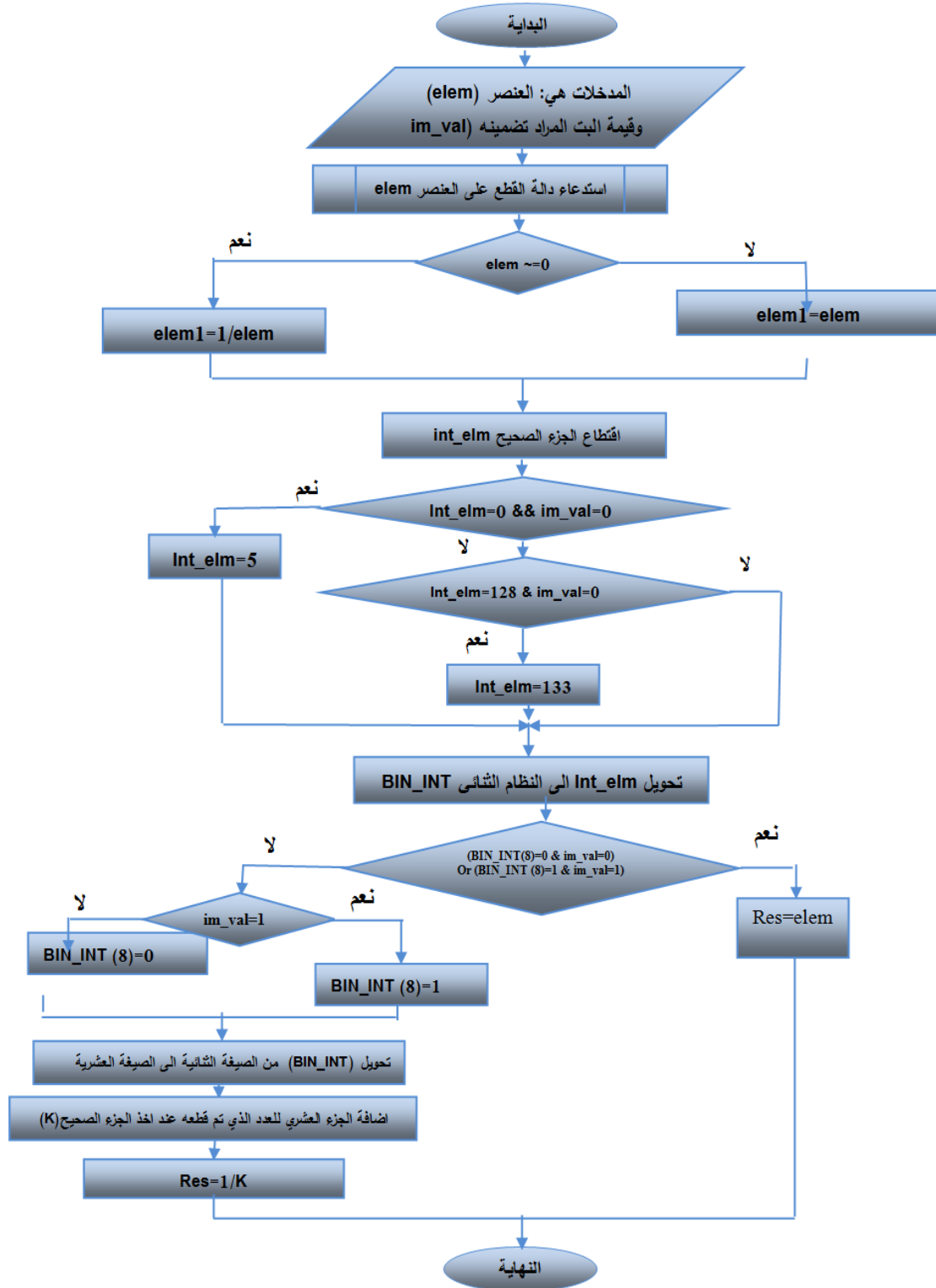
- خزن العينات الصوتية  $X_{11}$  داخل ملف من نوع wav.
- و الشكل (5،أ و ب) يوضح المخطط الانسيابي لأسلوب الإخفاء للطريقة المطورة. أما الشكل (6) فيوضح المخطط الانسيابي لدالة التضمين المستخدمة في الطريقة المطورة.



الشكل (5،أ و ب) مخطط انسيابي يوضح أسلوب الإخفاء للطريقة المطورة

- ب -





الشكل (6) مخطط انسيابي يوضح دالة التضمين للخوارزمية المطورة

## 2.7 خوارزمية الاسترجاع

**المدخلات:** الملف الحاوي على العلامة المائية المضمنة .

**المخرجات:** صورة العلامة المائية المسترجعة

**الخطوة الأولى:** إدخال اسم الملف الحاوي على العلامة المائية المضمنة، ثم قراءة محتويات الملف وخرن العينات الصوتية في مصفوفة  $x$ .

**الخطوة الثانية:** تقسيم الإشارة الصوتية  $x$  إلى مجموعة من القوالب (Frame) حيث كل قالب بحجم 512 عينة.

**الخطوة الثالثة:** تنفيذ الخطوات من 6-8 لخوارزمية الإخفاء على كل القوالب للملف بعد التضمين إلى ان تنتج لدينا المصفوفات  $U_w, S_w, V_w$

**الخطوة الرابعة:** استرجاع القيم الثنائية للعلامة المائية  $W(n)$  باستخدام مصفوفة  $V$ . حسب الأسلوب التالي:

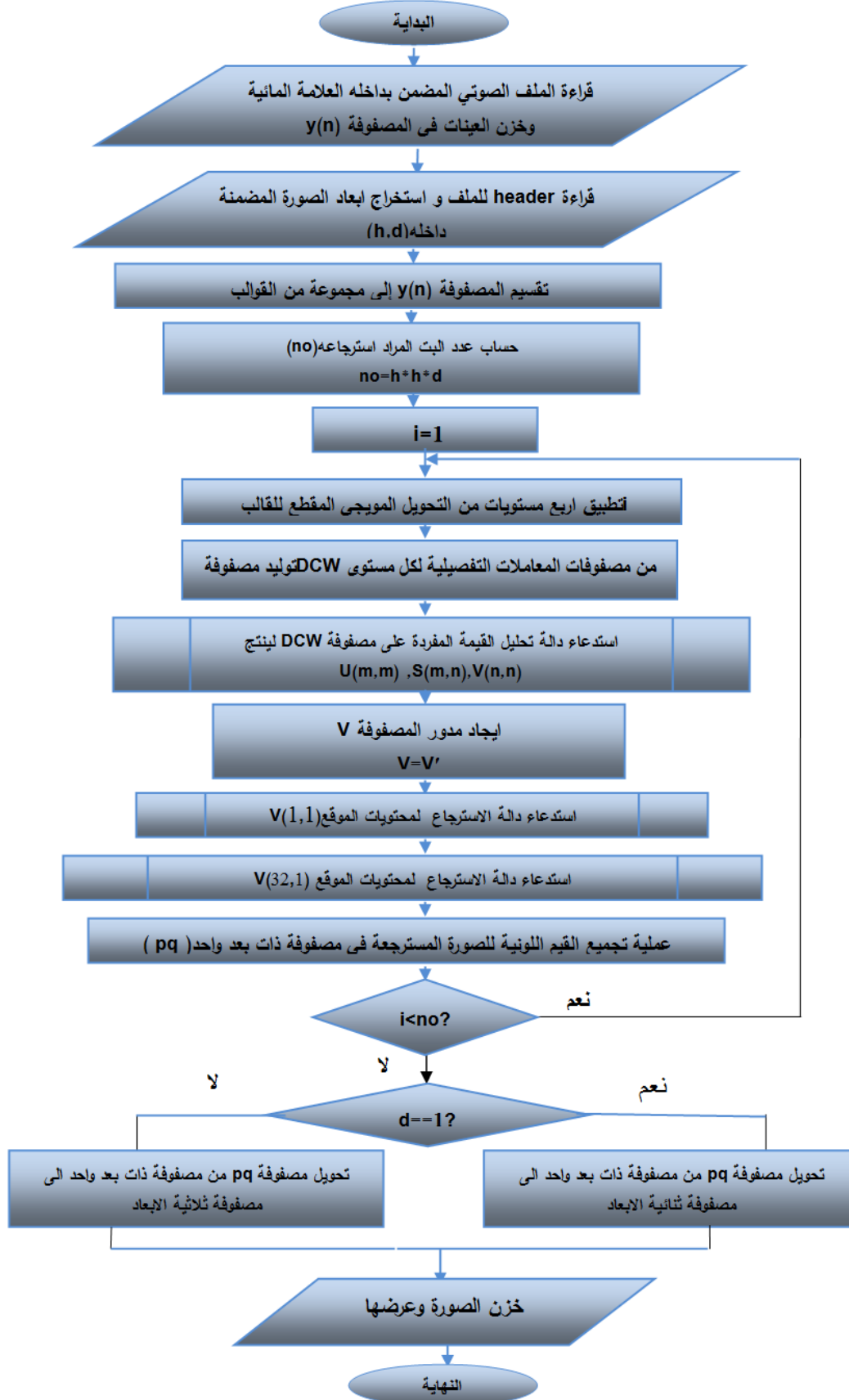
• تحديد المعامل  $V(i,j)$  حيث يتم إيجاد معكوس القيمة  $y = 1/V(i, j)$

• استرجاع القيمة الثنائية للعلامة المائية من البت الثامن للجزء الصحيح للعدد  $y$  الناتج من القسمة بعد

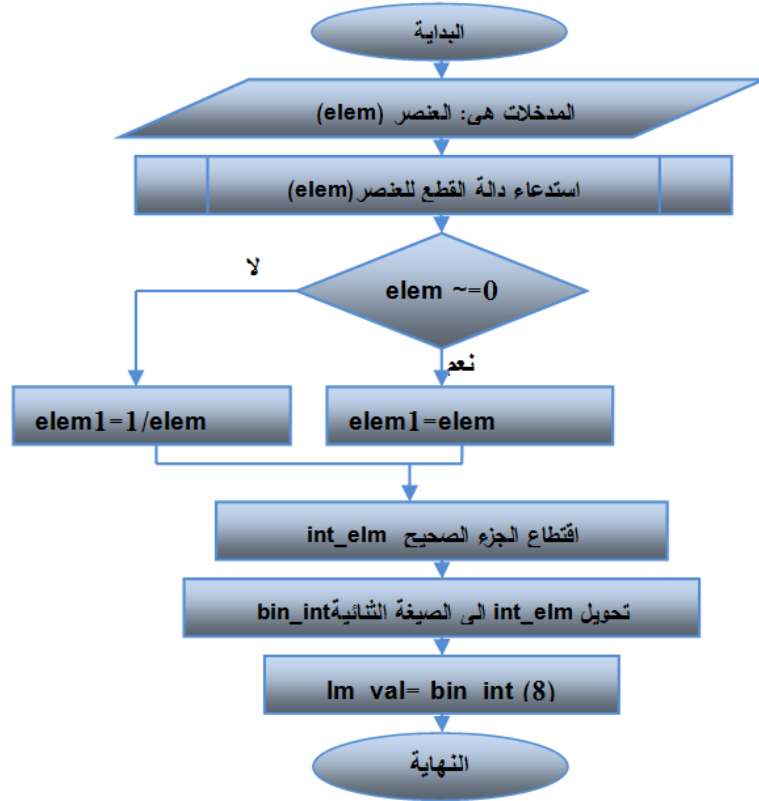
تحويله إلى الصيغة الثنائية.

**الخطوة الخامسة:** تحويل قيم الصورة من الثنائي إلى الصيغة العشرية. وتكوين الصورة وعرضها.

والشكل (7) يوضح المخطط الانسيابي لأسلوب الاسترجاع للطريقة المطورة. أما الشكل (8) فيوضح المخطط الانسيابي لدالة الاسترجاع المستخدمة في الطريقة المطورة.



الشكل (7) مخطط انسيابي يوضح أسلوب الاسترجاع للطريقة المطورة



الشكل (8) مخطط انسيابي يوضح دالة الاسترجاع للطريقة المطورة

## 8. قياس كفاءة الخوارزمية

### 1.8 قياس مقدار الاختلاف

يتم قياس كفاءة الخوارزمية من خلال تقييم ومقارنة جودة الكلام بعد إجراء المعالجة المطلوبة بواسطة بعض أنواع المقاييس، التي استخدمت نوعين من الاختبارات الشخصية والموضوعية ( Subjective and Objective Test). فالاختبارات الشخصية تستخدم الأذن البشرية في الإصغاء إلى الإشارة الأصلية والمضمنة من قبل عدد من الأشخاص، ويتم تقييم إشارة الكلام المضمنة عن طريق الاستماع إلى الإشارة المضمنة بدون الاستماع إلى الكلام الأصلي. ولنتمكن من تقييم مقدار الاختلاف يجب الاستماع إلى إشارة الكلام الأصلية والمسترجعة ثم مقارنة كليهما معاً. طبقاً لطبيعة الإذن البشرية فإن عملية التمييز بين الإشارة الأصلية والمضمنة تكون عملية صعبة، وغير موثوق بها وقلما تعطي تقييماً صحيحاً. لذلك يتم تقييم الكلام المشفر والمسترجع بالاعتماد على طريقة موثوق بها وهي الاختبارات الموضوعية (Test of Speech Signal Objective). لمعرفة مقدار التغيير الحاصل بين الإشارة الصوتية الناتجة بعد تضمين العلامة المائية والإشارة الصوتية الأصلية (إشارة الغطاء) يتم الاعتماد على المقاييس الموضوعية ومنها مقياس (SNR (signal to noise ratio)، حيث تعرف بأنها نسبة الاختلاف بين الإشارة الحاوية على ضوضاء والإشارة الأصلية. تسمى وحدة قياس SNR بالديسبل dB وتكون النسبة بين (30\_40db) هي نسبة جيدة وتعتبر هذه القيمة عن خاصية قدرة عدم الاكتشاف Undetected ability، يتم حسابها عن طريق المعادلة الآتية: [10]

$$SNR = \frac{1}{M} \sum_{m=1}^M 10 \log_{10} \frac{\sum_{n=1}^N |org\_sig(n)|^2}{\sum_{n=1}^N |wat\_sig(n) - org\_sig(n)|^2} \dots(4)$$

إذ أن : org\_sig : تحويل فورير للإشارة الأصلية ، Wat\_sig : تحويل فورير للإشارة المضمنة  
N : عدد عينات الكلام داخل المقطع ، M : عدد المقاطع

## 2.8 قياس جودة العلامة المائية المسترجعة

يتم حساب نسبة التطابق بين صورة العلامة المائية الأصلية والمسترجعة بالاعتماد على معامل الارتباط correlation factor، حيث الارتباط هو مقياس لقوة العلاقة بين المتغيرات العشوائية، إن معامل الارتباط بين اثنين من المتغيرات (X) و (Y) معرف كما يأتي:

$$\rho(X, Y) = \text{Covariance}(X, Y) / \{\text{Variance}(X) \times \text{Variance}(Y)\}^{1/2} \dots(5)$$

حيث إن (ρ) هو معامل الارتباط، وهو العدد الذي يُلخّص الاتجاه وقرب العلاقات الخطية بين متغيرين. ومعامل الارتباط يُمكن أن يأخذ القيم بين (-1 و +1) والإشارة (+ أو -) لمعامل الارتباط تمثل اتجاه العلاقة. والجدول (1) يصف القوة والاتجاه لقيم معامل الارتباط. [11]

الجدول (1) قوة واتجاه قيم معامل الارتباط

الاتجاه	القوة	معامل الارتباط(P)
+	علاقة خطية مثالية	P = 1
+	علاقة خطية قوية جداً	1 > P >= 0.9
+	علاقة خطية قوية	0.9 > P >= 0.7
+	علاقة خطية متوسطة	0.7 > P >= 0.5
+	علاقة خطية ضعيفة	0.5 > P >= 0.3
+	علاقة خطية ضعيفة جداً	0.3 > P > 0
	لا توجد علاقة	P = 0
-	علاقة خطية ضعيفة جداً	0 > P > -0.3
-	علاقة خطية ضعيفة	-0.3 >= P > -0.5
-	علاقة خطية متوسطة	-0.5 >= P > -0.7
-	علاقة خطية قوية	-0.7 >= P > -0.9
-	علاقة خطية قوية جداً	-0.9 >= P > -1
-	علاقة خطية مثالية	P = -1

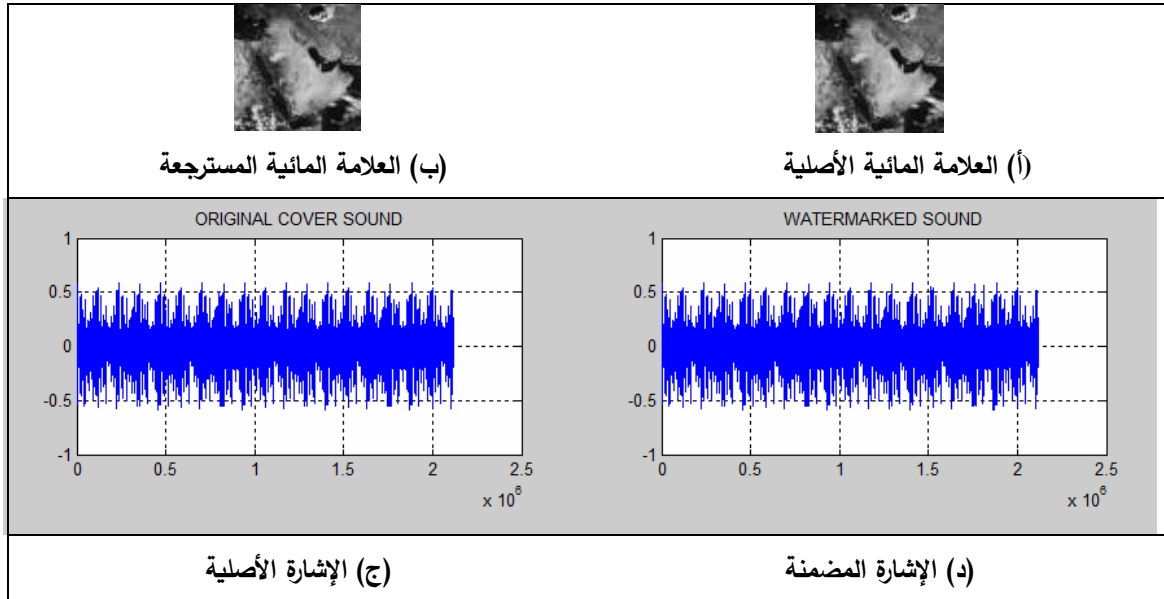
## 9. مناقشة النتائج

أجريت اختبارات متعددة على الخوارزمية المطورة لتضمين صورة مختلفة الأبعاد رمادية وملونة وبالامتدادين BMP وJPG، إذ أن الامتداد الأول هو صيغة للصور الرقمية غير المكبوسة، والامتداد الثاني هو صيغة مكبوسة كبسا بفقدان. وكانت نتائج التضمين والاسترجاع للصورة في الإشارة الصوتية كما هو مبين في الجدول (2).

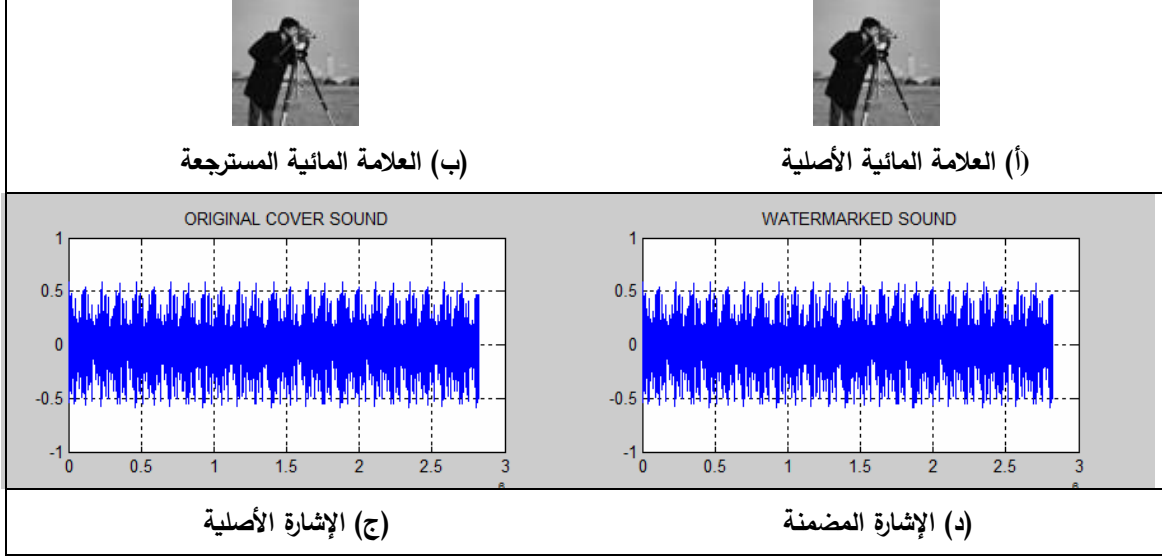
الجدول (2) نتائج التضمين للخوارزمية المطورة

قياس كفاءة الخوارزمية		حجم العلامة المائية	حجم الغطاء	صورة العلامة المائية	الملف الصوتي (الغطاء)
CORR الصورة الأصلية/الصورة المسترجعة	SNR الإشارة الأصلية/الإشارة المضمنة				
1	41.0049	64*64*1	8.06 MB	L_map.bmp	Loopmusic1.wav
1	30.41	64*64*1	8.06 MB	Cameraman.bmp	Loopmusic1.wav
0.87431	28.2127	21*21*3	5.509KB	Children.bmp	Loopvlong.wav
0.95258	29.4931	30*30*3	8.06 KB	Swar117.jpg	Loopmusic1.wav
0.9756	29.6421	21*21*3	5.509KB	Smallimage.jpg	Loopvlong.wav

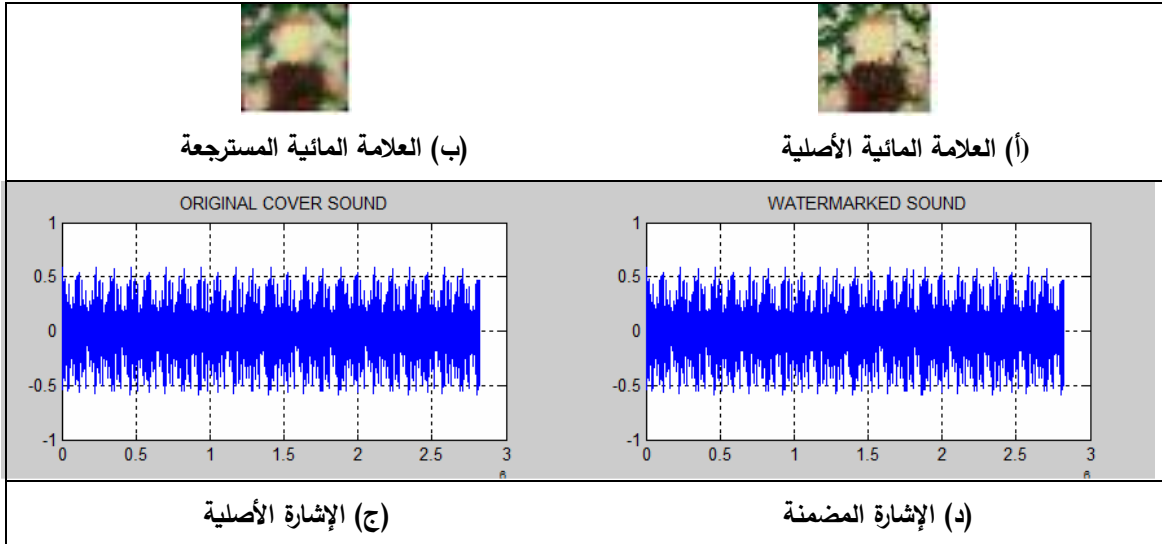
ويبين الجدول (2) قياس مقدار الاختلاف بين الإشارة الأصلية والإشارة بعد التضمين حسب المعادلة (2) كانت جيدة ونسبة الضوضاء قليلة، أما قيمة معامل الارتباط بين الصورة الأصلية والصورة المسترجعة حسب المعادلة (3) فإن النتيجة كانت جيدة وهي علاقة خطية قوية جداً حسب الجدول (1). يوضح الشكل (9)، (10) و(11) أنموذجاً لصورة رمادية وملونة من الصور التي تم التطبيق عليها.



الشكل (9) تضمين صورة رمادية (L\_map.bmp) في إشارة صوتية (loopmusic1.wav)



الشكل (10) تضمين صورة رمادية (cameraman.bmp) في إشارة صوتية (loopmusic1.wav)



الشكل (11) تضمين صورة ملونة (Swar117.jpg) في إشارة صوتية (loopmusic1.wav)

ولتقييم القوة (Robustness) للطريقة المطورة للإخفاء أمام الهجمات عليها واكتشاف البيانات المخفية أو تدميرها و تشويشها تم تعريض إشارة الصوت المضمنة بداخلها العلامة المائية إلى العديد من الهجمات ومن ثم تم قياس مقدار معامل الارتباط بين الصورة الأصلية والصورة المسترجعة وفيما يلي عرض لأنواع الهجمات التي تم تنفيذها على الإشارة المضمنة بداخلها العلامة المائية.

1. إضافة الضوضاء (Add noise) : تم إضافة سلسلة من الضوضاء البيضاء (white noise) إلى الإشارة بالشكل الآتي:

$$Z'(n) = x'(n) + A \cdot g(n) \quad \dots(6)$$




إذ أن  $g(n)$  تمثل سلسلة الضوضاء البيضاء (White Noise Sequence) ،  $A$  تمثل ثابت (حيث أن قيمة  $A=0.08$  ،  $x'(n)$  تمثل الإشارة المضمنة بداخلها العلامة المائية.

2. التضخيم (Amplify) : توسيع سعة (Amplitude) الإشارة المضمن بداخلها العلامة المائية.

3. zero cross : تصفير قيم العينات الأقل من قيمة عتبة معينة.

والجدول (3) يعرض الصورة المسترجعة بعد تعريض الإشارة إلى الهجمات المذكورة سابقاً. وكذلك يبين نسبة معامل الارتباط.

الجدول (3) نتائج الصورة المسترجعة بعد تعريض الإشارة الصوتية إلى الهجمات

قياس جودة الصورة المسترجعة	صورة العلامة المائية المسترجعة	نوع الهجوم
CORR الصورة الأصلية/الصورة المسترجعة		
0.97551		Add noise
0.97448		Zero cross
0.91486		Amplitude

## 9. الاستنتاجات

تم التوصل إلى الاستنتاجات الآتية:-

1. يمكن زيادة عدد البت المراد إخفاؤها وذلك بتقليل حجم القالب مما يؤدي إلى زيادة عدد القوالب، حيث ان عدد البت الممكن إخفاؤها يعتمد على عدد القوالب.
2. على الرغم من استخدام DWT (حيث يحقق التحويل المويجي كبس بفقدان ) و التي تحقق نسبة كبس للإشارة إلى النصف في كل مستوى من المستويات الأربعة التي تم تطبيقها إلا أننا تمكنا من استرجاع الصورة بنسبة جيدة .
3. التضمين في عناصر المصفوفة V يعطي قوة أكثر (robustness) ضد الضوضاء من التضمين في العناصر القطرية للمصفوفة S المطبق في بحوث أخرى.
4. إن تأثير حدوث الخطأ (في حالة حصوله) في الصورة الملونة ممكن أن يكون كبيراً حسب موقع البت حيث أن القيمة اللونية للصورة الملونة تمثل ب(24) بت. ومن خلال التطبيق العملي لاحظنا استرجاع الصورة الملونة بصورة جيدة حيث إن معامل الارتباط المحسوب يمثل علاقة خطية قوية جداً وهذا دليل على أن نسبة الخطأ في قيم البت المسترجع قليل جداً ويكاد يكون معدوماً.
5. على الرغم من الإخفاء في الخلية الثنائية الأعلى أهمية MSB داخل العنصر للمصفوفة V فان قيمة SNR بين الإشارة الأصلية والإشارة بعد التضمين و حسب الجدول رقم(2) المبين سابقاً كانت جيدة.

6. نتائج الخوارزمية بعد تطبيق عدد من الهجمات على الإشارة المضمنة كانت جيدة كما مبين في الجدول رقم (3) وهذا يدل على قوة الخوارزمية المطورة.

#### 10. الأعمال المستقبلية

1. يمكن تطبيق الخوارزمية المطورة على ملفات الفيديو(الغطاء).
2. تشفير العلامة المائية قبل إجراء عملية التضمين لزيادة السرية.
3. إجراء اتصال غير مرئي بين طرف المرسل والمستلم باستخدام القنوات المخفية للتقليل من مستوى الشك في وجود اتصال سري.

المصادر

- [1] الحمامي، علاء حسين و الحمامي، محمد علاء (2008)، "إخفاء المعلومات: الكتابة المخفية والعلامة المائية"، إثراء للنشر والتوزيع، الشارقة.
- [2] العلي، فرح طارق محمد (2004)، "حماية استنساخ الكتابة باستخدام انتشار الطيف"، رسالة ماجستير غير منشورة، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.
- [3] Al\_Haj Ali, and Mohammad Ahmad, (2010), "Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition", European Journal of Scientific Research, ISSU 1450-216X Vol. 39 No1,pp. 6-21.
- [4] Ali, Dujan Basheer Taha, (2004), " Digital Image Watermarking Techniques for Copyright Protection ", Unpublished D. Ph. Thesis, University of Mosul, Iraq.
- [5] Amansouri, A mahmoudi Aznavah and Ftorkamani , (2009), " SVD\_Based Digital Image Watermarking Using Complex Wavelet Transform ", Sadhaua Vol. 34,part3,PP. 393\_406© printed in India.
- [6] Chandra DVS,( 2002)," Digital image watermarking using singular value decomposition ",IEEE Midwest Symposium on Circuits and Systems Tulsa Oklahoma,III 264–III 267.
- [7] Donaied G.Children, (2000), " Speech Processing and Synthesis Tool Boxes ", United States of America.
- [8] Kashiappa Aditya,( 2010), " Acclerating Watermarking in SVD Domain Using Graphic Processing Units ", M.Sc Thesis, Unversity Massachusetts Dartmouth.
- [9] Rocha A., and Goldenstein S., (2008), " *Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?*", RITA,Vol. 15, No. 1,pp. 83-110.
- [10] Saffor, Amhamed and Ramli, Abdul Rahman, (2001), "A Comparative Study of Image Compression between JPEG and Wavelet", University Putra Malaysia, vol. 14, no. 1, 2001, pp. 39-45, Selangor, Malaysia.
- [11] Shen. D, Lu. Z & Pharmaceuticals. A, "Computation of Correlation Coefficient and Its Confidence Interval in SAS", Paper 170-31, [www.sas.com/proceedings/sugi31/170-31.pdf](http://www.sas.com/proceedings/sugi31/170-31.pdf).
- [12] Wu,Y, (2009) , "on the Security of SVD\_Based Ownership Watermarking", Multimedia 7,PP. 624\_627.