Ministry of Higher Education
And Scientific Research
University of Technology
Department of computer science

Image Encryption Using Substitution-Permutation Network with Chaotic Mapping

A Dissertation

Submitted to the Department of Computer Scienceof the University of TechnologyIn Partial Fulfillment of the Requirements for theDegree of Doctor of Philosophy in Computer science

By

Ekhlas Abbas JaberAlbaharany

Supervised by

Prof. Dr. HilalHadiSaleh Asst. Prof Dr.LumaFayeqJalil

December \ 2015 **Safar / 1437**

جمهورية العراق
وزارة التعليم العالي والبحث العلم
الجامعة التكنولوجية
قسم علوم الحاسبات

تشفير الصورةباستخدام شبكة التعويض الابدالي مع العلاقات الفوضوية

اطروحة مقدمة الى قسم علوم الحاسبات في الجامعة التكنولوجية
وهي جزء من متطلبات نيل شهادة الدكتوراة في علوم الحاسبات

من قبل

إخلاص عباس جبر البحراني

باشراف

أ.د هلال هادي صالح د.لمى فايق جليل

صفر \ 1437 كانون الاول \ 2015

المستلخص

نظرية الفوضى تمتلكالعديد من خصائص مثل انها تبين إحصاءات متماثلة عندما يقاس على مدى الزمان أو المكان , الاختلاط، العشوائية ، لا يمكن التنبؤ به والحساسية للقيم الابتدائية, يمكن ان نربطها مع خاصيتين معروفتين من خصائص انظمة التشفير الكلاسيكية هما التشويش والنشر.

لذلك فيهذه الأطروحة، تم تصميمخوارزمية جديدة لتشفيرالصورعن طريق المزج بين التشفير الكتلي ونظرية الفوضى. الخوارزمية المقترحة تقوم بتشفير /تحليل كتلة مكونة من 256 بايت.عملية تصميم نظام التشفير المقترح قد تم تقسمها إلى تصميمثلاث اجزاء رئيسية للخوازمية المقترحة وهي:

اولا تصميم مولد أرقام عشوائية جديد يطلق عليه مولد الارقام(بت)العشوائي الفوضوي (CRNG) والذي يستخدم لتوليد سلسلة من الأرقام أو بت تخدم كمفتاح للالخوارزمية المقترحة.CRNGيعتمد علىمعادلة تحويل جاكوبي ومعادلة التحويل القياسية للفوضى.***ثانيا*** تصميم جزء الاستبدال الغير الخطي-S box الذي يستخدم في الخوارزمية المقترحة والذياطلق عليه الاستبدال غير المباشرة الفوضوي الديناميكي المستقل المفتاح (CDKDS-box) باستخدام معادلة كروس والمعادلة اللوجستية للفوضى حيث ان S-box هي جدول 16 × 16 من قيم الأعداد الصحيحة (256 بايت). أكثر ال S-box الموجودة تستبدل البايت باخر جديد بالاعتماد مباشرة على أرقام الصفوف والأعمدة. في CDKDS-box المقترح ، كل بايت اولايحول الى بايت اخر ومن ثم ناخذ البايت الجديد منCDKDS-box.

ثالثا هيتصميمخوارزمية التشفيروفك التشفير للخوارزمية SPN لتشفير النص والصورة الكتلية الفوضوية التي تشفر وتحلل كتلة مكونة من 256 بايت.تتالف الخوارزمية من 10 دورات. كل دورة تستخدم S-box واحد هذا يعني انه بعد كل دورة فان ترتيب عناصر ال S-box يتم اعادة ترتيبها باستخدم معادلة بيكر الفوضوية. وتم تحليل الاداء للسلاسل الناتجة عن المولد المقترح من خلالاستخدام الحزمة الإحصائيةNISTوأيضاالأساليب الإحصائية التقليدية. جميعالسلاسلالمفحوصة(مفردةومدمجة) اجتازت الاختباراتNISTبنجاحمن حيث انηتمثل نسبةالنجاحللسلاسلالفردية والتي يجب ان تكونبين[0.984 0.995] وp-valueتمثل نسبةالنجاحللسلاسلالمدمجةوالتي يجب ان تكونبين[0.04090..0.9996]. الارتباط بين كل السلاسل المولدة تم اختبارها من خلال احتساب معامل ارتباط بيرسون و مسافة هامينك . توزيعات معاملاتارتباط بيرسونتنتمي إلى[-0.08، 0.08] التيهي قريبةجداإلى 0والتوزيعات معاملاتمسافة هامينك ينتمي إلى [0.465، 0.535] التي هيقريبة جدا من القيمة المثالية0.5. وهذا يعنيأن العلاقةبينالسلاسلالمتولدةصغير جدا. كمايتم اختبارCRNGالمقترحةباستخدام نفسمعاملاتوجدنا أن لديهاحساسيةعالية للمفاتيح. وأخيراCRNGالمقترحيسمح بمقاومةالهجماتالتفاضلية والغاشمة هجومالقوةحيث انالمساحة الإجماليةللمفتاح في CRNGالمقترح هو2^{160}+2^{24}. كما تم تحليل الاداء لل S-Box المقترح عن طريق بناء100CDKDS-boxمنمفاتيحقريبةأومتتاليةواختبارهاباستخداممعاييرS-box الجيدة.جميع S-

boxesتمتلك القدرة على مقاومة مهاجمةالقتران التناظريومهاجمة تأثير الانهيار. كلS-100 boxesلديهامعيار الانهيار الصارم SACممتازلأنالقيمة المتوسطةلكل مصفوفات الاعتماد تقعفي [0.46، 0.53]، والتي هي قريبة منقيمةمثالية0.5. كلS-boxes100لديهامناعةجيدة ضدالهجماتالتفاضلية وغير خطية حيثتقعكلالقيمداخل[256/10، 256/12] والتي هيأيضا على مقربة منقيمةمثاليةومعدلكلالقيمهو 0.0760089. من خلال حسابمعامل الارتباطبينS-boxes المكونة، وجدنا أنS-boxesحساسة جدا للمفاتيح. واخيرا تم قياس أداء خوارزمية التشفير المقترحة الكاملة من خلال سلسلة من الاختبارات التي أجريت على صور مختلفة. وقد أظهرت النتائج التجريبية ونتائج المقارنة أن الخوارزمية المقترحة لها فضاء أعلى تقريبا (2^{266}) مقارنة مع خوارزميات أخرى والذي يدل على أن لديها القدرة على مقاومة هجوم الغاشمة وهجوم القوة. كان لديه أدنى قيمة لترابط، قيمة الانتروبي أعلى، والرسم البياني أكثر اتساقا. فمن حساسية عالية للوصول إلى المفتاح التي تظهر أن لديها القدرة على معارضة هجوم شامل. وبالإضافة إلى ذلك، الخوارزمية المقترحةلديهاالقدرةعلى مقاومةالهجومالنص الصريح المعروف، وهجوم اختيار النص الصريح والهجومالتفاضلية. وبالتالي فإن خوارزمية SPN لتشفير النص والصورة الكتلية الفوضوية المقترحة لديها جودة عالية التشفير لأن جميع الصور لها قيم عالية لأقصى قدر من الانحراف، وانخفاض قيمة الغيرالنظامية وانخفاض قيمة نسبة الذروة الإشارة إلى الضوضاء.

.

Abstract

Chaos theory has many characteristics of, such as ergodicity, mixing, randomness, unpredictability and the sensitivity to initial conditions which can be connected with the well-known confusion and diffusion properties in the classical cryptography. So, new image encryption algorithm based on a combination between Substitution-Permutation Networks (SPN)block cipher and chaotic mapping is proposed in this dissertation.The proposed cipher encrypts/decrypts block of 256 (16 × 16) bytes. The designing process has beensplit into the design of three main parts needed for proposed cipher system which are ***First*** is the design of newpseudo-random numbers generator called **Chaotic Random Number (bit) Generator (CRNG)**that is used to generate sequence of numbers or bitsserving as the key for the proposed algorithm. CRNG is based on the Jacobian elliptic chaotic maps and Standard map. ***Second*** is the design of thenonlinear substitution componentin the proposed cipher which is called **Chaotic Dynamical Key Dependent S-boxes (CDKDS-box)** based on 2D Cross map and 2D Logistic mapproposed. CDKDS-box is a table of 16 × 16 integer values (256 bytes). Most of existing S-box substitute byte into new byte based on the row and column numbers directly. In the proposed CDKDS-box, each individual byte of state is first diffused to another byte and then substitutedinto a new byte from CDKDS-box. ***Third***is the design of **the encryption and decryption algorithm of the chaotic block SPN image cipher algorithm**which encrypts and decrypts a block of 256 byte. The algorithm consists of 10 rounds.One S-Box for a round. This means that after each round, the S-box is permuted using chaotic Baker map.

The performance of the sequences generated by the CRNGis analyzed through the National Institute of Standards and Technology(NIST) statistical package and conventional statistical methods. All the tested sequences have passed successfully the NIST tests where the ratio η of p-value concerns individual sequences between [0.984.. 0.995] and the p-value concerns the concatenate sequences between [0.04090.. 0.9996]. The correlation between the produced sequences is very small where the correlation is computed by Pearson's correlation coefficient and Hamming distance. The distributions of Pearson's correlation coefficients belong to [-0.08, 0.08] which are very close to 0 and the distributions of Hamming distance coefficients belonging to [0.465, 0.535] which are very close to ideal value of 0.5. Also, the sensitivity of the proposed CRNG to the keys is tested using the same coefficients and

it is found that it is verysensitive to the keys. Lastly the proposed CRNG allows resisting the differential attacks and brute force-attack where the total space of keys of proposed CRNG is $2^{160}+2^{24}$.

The performance of proposedCDKDS-Boxis analyzed by constructing 100 CDKDS-Box from nearby or successive keys and tested usingthe criteria for good S-box. All the S-boxes are fulfilling bijective property and the avalanche effect. All the 100 S-boxes have excellent Strict Avalanche Criteria(SAC) because the entire mean values of the dependence matrixes are located within [0.46, 0.53], which are close to the ideal value of 0.5. All the 100 S-boxes have good immunity against differential probability (DP) and linear probability (LP) attacks where all the DPs values are located within [10/256, 12/256] which are also close to the ideal value and the average of all LPs values is 0.0760089. By computing the correlation coefficient between the created S-box, we found that the S-boxes are very sensitive to the keys.

The performance of proposed algorithm is measured through a number of tests on different images.The experimental results and comparative results have shown that the proposed algorithm has higher key space (2^{266}) than other compared algorithms which demonstrates it has the ability of resisting brute force-attack. It has lower correlation, a higher entropy value, and a more uniform histogram. It’s high sensitivity to the keyshows that it has the ability of opposing exhaustive attack. In addition, the proposed algorithm has the ability of resisting the known-plaintext attack, the chosen-plaintext attack and the differential attack. Lastly the chaotic block SPN image and text cipher algorithm havehigh encryption quality because all tested images have high value for maximum deviation, low irregular value and low Peak Signal-to-Noise Ratio value.

Abstract

Chaos theory has many characteristics of, such as ergodicity, mixing, randomness, unpredictability and the sensitivity to initial conditions which can be connected with the well-known confusion and diffusion properties in the classical cryptography. So, new image encryption algorithm based on a combination between Substitution-Permutation Networks (SPN) block cipher and chaotic mapping is proposed in this dissertation. The proposed cipher encrypts/decrypts block of 256 (16 × 16) bytes. The designing process has been split into the design of three main parts needed for proposed cipher system which are ***First*** is the design of new pseudo-random numbers generator called **Chaotic Random Number (bit) Generator (CRNG)** that is used to generate sequence of numbers or bits serving as the key for the proposed algorithm. CRNG is based on the Jacobian elliptic chaotic maps and Standard map. ***Second*** is the design of the nonlinear substitution component in the proposed cipher which is called **Chaotic Dynamical Key Dependent S-boxes (CDKDS-box)** based on 2D Cross map and 2D Logistic map proposed. CDKDS-box is a table of 16 × 16 integer values (256 bytes). Most of existing S-box substitute byte into new byte based on the row and column numbers directly. In the proposed CDKDS-box, each individual byte of state is first diffused to another byte and then substituted into a new byte from CDKDS-box. ***Third*** is the design of **the encryption and decryption algorithm of the chaotic block SPN image cipher algorithm** which encrypts and decrypts a block of 256 byte. The algorithm consists of 10 rounds. One S-Box for a round. This means that after each round, the S-box is permuted using chaotic Baker map.

The performance of the sequences generated by the CRNG is analyzed through the National Institute of Standards and Technology (NIST) statistical package and conventional statistical methods. All the tested sequences have passed successfully the NIST tests where the ratio η of p-value concerns individual sequences between [0.984.. 0.995] and the p-value concerns the concatenate sequences between [0.04090.. 0.9996]. The correlation between the produced sequences is very small where the correlation is computed by Pearson's correlation coefficient and Hamming distance. The distributions of Pearson's

correlation coefficients belong to [-0.08, 0.08] which are very close to 0 and the distributions of Hamming distance coefficients belonging to [0.465, 0.535] which are very close to ideal value of 0.5. Also, the sensitivity of the proposed CRNG to the keys is tested using the same coefficients and it is found that it is very sensitive to the keys. Lastly the proposed CRNG allows resisting the differential attacks and brute force-attack where the total space of keys of proposed CRNG is $2^{160}+2^{24}$.

The performance of proposed CDKDS-Box is analyzed by constructing 100 CDKDS-Box from nearby or successive keys and tested using the criteria for good S-box. All the S-boxes are fulfilling bijective property and the avalanche effect. All the 100 S-boxes have excellent Strict Avalanche Criteria (SAC) because the entire mean values of the dependence matrixes are located within [0.46, 0.53], which are close to the ideal value of 0.5. All the 100 S-boxes have good immunity against differential probability (DP) and linear probability (LP) attacks where all the DPs values are located within [10/256, 12/256] which are also close to the ideal value and the average of all LPs values is 0.0760089. By computing the correlation coefficient between the created S-box, we found that the S-boxes are very sensitive to the keys.

The performance of proposed algorithm is measured through a number of tests on different images. The experimental results and comparative results have shown that the proposed algorithm has higher key space (2^{266}) than other compared algorithms which demonstrates it has the ability of resisting brute force-attack. It has lower correlation, a higher entropy value, and a more uniform histogram. It's high sensitivity to the key shows that it has the ability of opposing exhaustive attack. In addition, the proposed algorithm has the ability of resisting the known-plaintext attack, the chosen-plaintext attack and the differential attack. Lastly the chaotic block SPN image and text cipher algorithm have high encryption quality because all tested images have high value for maximum deviation, low irregular value and low Peak Signal-to-Noise Ratio value.

المستلخص

نظرية الفوضى تمتلك العديد من خصائص مثل انها تبين إحصاءات متماثلة عندما يقاس على مدى الزمان أو المكان , الاختلاط، العشوائية ، لا يمكن التنبؤ به والحساسية للقيم الابتدائية, يمكن ان نربطها مع خاصيتين معروفتين من خصائص انظمة التشفير الكلاسيكية هما التشويش والنشر.

لذلك في هذه الأطروحة، تم تصميم خوارزمية جديدة لتشفيرالصورعن طريق المزج بين التشفير الكتلي ونظرية الفوضى. الخوارزمية المقترحة تقوم بتشفير / تحليل كتلة مكونة من 256 بايت.

عملية تصميم نظام التشفير المقترح قد تم تقسمها إلى تصميم ثلاث اجزاء رئيسية للخوازمية المقترحة وهي :

اولا تصميم مولد أرقام عشوائية جديد يطلق عليه مولد الارقام (بت) العشوائي الفوضوي (CRNG) والذي يستخدم لتوليد سلسلة من الأرقام أو بت تخدم كمفتاح للالخوارزمية المقترحة. CRNG يعتمد على معادلة تحويل جاكوبي ومعادلة التحويل القياسية للفوضى. ***ثانيا*** تصميم جزء الاستبدال الغير الخطي S-box الذي يستخدم في الخوارزمية المقترحة والذي اطلق عليه الاستبدال غير المباشرة الفوضوي الديناميكي المستقل المفتاح (CDKDS-box) باستخدام معادلة كروس والمعادلة اللوجستية للفوضى حيث ان S-box هي جدول 16 × 16 من قيم الأعداد الصحيحة (256 بايت). أكثر ال S-box الموجودة تستبدل البايت باخر جديد بالاعتماد مباشرة على أرقام الصفوف والأعمدة. في CDKDS-box المقترح ، كل بايت اولا يحول الى بايت اخر ومن ثم ناخذ البايت الجديد من CDKDS-box. ***ثالثا*** هي تصميم خوارزمية التشفير وفك التشفير للخوارزمية SPNلتشفير النص والصورة الكتلية الفوضوية التي تشفر وتحلل كتلة مكونة من 256 بايت. تتالف الخوارزمية من 10 دورات. كل دورة تستخدم S-box واحد هذا يعني انه بعد كل دورة فان ترتيب عناصر ال S-box يتم اعادة ترتيبها باستخدم معادلة بيكر الفوضوية.

وتم تحليل الاداء للسلاسل الناتجة عن المولد المقترح من خلال استخدام الحزمة الإحصائيةNIST وأيضا الأساليب الإحصائية التقليدية. جميع السلاسل المفحوصة (مفردة ومدمجة) اجتازت الاختبارات NIST بنجاح من حيث ان η تمثل نسبة النجاح للسلاسل الفردية والتي يجب ان تكون بين [0.984 0.995] وp-value تمثل نسبة النجاح للسلاسل المدمجة والتي يجب ان تكون بين [0.04090.. 0.9996]. الارتباط بين كل السلاسل المولدة تم اختبارها من خلال احتساب معامل ارتباط بيرسون و مسافة هامينك . توزيعات معاملات ارتباط بيرسون تنتمي إلى [-0.08، 0.08] التي هي قريبة جدا إلى 0 والتوزيعات معاملات مسافة هامينك ينتمي إلى [0.465، 0.535] التي هي قريبة جدا من القيمة المثالية 0.5. وهذا يعني أن العلاقة بين السلاسل المتولدة صغير جدا. كما يتم اختبار CRNG المقترحة باستخدام نفس معاملات وجدنا أن لديها حساسية عالية للمفاتيح.

وأخيرا CRNG المقترح يسمح بمقاومة الهجمات التفاضلية والغاشمة هجوم القوة حيث ان المساحة الإجمالية للمفتاح في CRNG المقترح هو $2^{160} + 2^{24}$. كما تم تحليل الاداء لل S-Box المقترح عن طريق
بناء 100 CDKDS-box من مفاتيح قريبة أو متتالية واختبارها باستخدام معايير S-box الجيدة . جميع S-boxes تمتلك القدرة على مقاومة مهاجمة القران التناظري ومهاجمة تأثير الانهيار. كل 100 S-boxes لديها معيار الانهيار الصارم SAC ممتاز لأن القيمة المتوسطة لكل مصفوفات الاعتماد تقع في [0.46، 0.53]، والتي هي قريبة من قيمة مثالية 0.5. كل 100 S-boxes لديها مناعة جيدة ضد الهجمات التفاضلية وغير خطية حيث تقع كل القيم داخل [256/10، 256/12] والتي هي أيضا على مقربة من قيمة مثالية ومعدل كل القيم هو 0.0760089. من خلال حساب معامل الارتباط بين S-boxes المكونة، وجدنا أن S-boxes حساسة جدا للمفاتيح. واخيرا تم قياس أداء خوارزمية التشفير المقترحة الكاملة من خلال سلسلة من الاختبارات التي أجريت على صور مختلفة. وقد أظهرت النتائج التجريبية ونتائج المقارنة أن الخوارزمية المقترحة لها فضاء أعلى تقريبا (2^{266}) مقارنة مع خوارزميات أخرى والذي يدل على أن لديها القدرة على مقاومة هجوم الغاشمة وهجوم القوة. كان لديه أدنى قيمة لترابط، قيمة الانتروبي أعلى، والرسم البياني أكثر اتساقا. فمن حساسية عالية للوصول إلى المفتاح التي تظهر أن لديها القدرة على معارضة هجوم شامل.
وبالإضافة إلى ذلك، الخوارزمية المقترحة لديها القدرة على مقاومة الهجوم النص الصريح المعروف، وهجوم اختيار النص الصريح والهجوم التفاضلية. وبالتالي فإن خوارزمية SPN لتشفير النص والصورة الكتلية الفوضوية المقترحة لديها جودة عالية التشفير لأن جميع الصور لها قيم عالية لأقصى قدر من الانحراف، وانخفاض قيمة الغيرالنظامية وانخفاض قيمة نسبة الذروة الإشارة إلى الضوضاء.

.