سال ششم، شماره‌های ۱۹ و ۲۰، بهار و تابستان ۱۳۹۳
صص: ۴۱-۵۸

فصلنامهٔ علمی- پژوهشی
فناوری اطلاعات و ارتباطات ایران

مطالعه‌ای بر رمزنگاری بصری و ارائهٔ روش پیشنهادی برای رمزنگاری تصاویر رنگی

شهریار محمدی* نغمه محمدی**
*استادیار، گروه فناوری اطلاعات، دانشکدهٔ صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران
**کارشناس ارشد، فناوری اطلاعات، دانشکدهٔ صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران

تاریخ دریافت: ۱۳۹۲/۷/۲۷ تاریخ پذیرش: ۱۳۹۲/۱۲/۹

چکیده

رمز نگاری بصری روشی است که از ویژگی‌های دید انسان استفاده می‌نماید و به دانش رمزنگاری و محاسبات پیچیده نیاز ندارد و پیاده‌سازی آن ساده است. مدل‌کاهشی، مدلی است که در آن، رنگ‌ها با استفاده از ترکیبی از پرتوهای منعکس شده از اجسام نمایش داده می‌شوند، با مخلوط فیروزه‌ای،سرخابی و زرد طیف گسترده‌ای از رنگ‌ها ایجاد می‌شود. واقعیت آن است که باوجود معرفی روش‌ها و الگوریتم‌های گوناگون در زمینهٔ رمزنگاری، این روش‌ها همچنان نتواسته‌اند تا حدّ قابل قبولی رضایت کاربران را از امنیت سیستم‌ها فراهم آورند. . این مقاله بر آن است که در عین مرور روش‌های گوناگون رمزنگاری بصری، روش‌های رمزنگاری بصری پیشنهادی خود را برای تصاویر رنگی ارائه نماید که تصویر رنگی را بعد از تبدیل به تصاویر هالفتون بر اساس رمزنگاری بصری سیاه و سفید به بخش‌هایی تقسیم می‌نماید و قوانین آن طبق مدل‌کاهشی رنگ‌ها است.

واژه‌های کلیدی: رمزنگاری بصری،اشتراک‌گذاری مخفیk از n ، هالفتون

مقدمه

رمز نگاری بصری[1] توسط شمیر[2] و نیور[3] معرفی شده است که برای به رمز در آوردن مواد نوشته شده مانند: متن چاپی، دست نوشته، عکس و غیره استفاده می‌شود [۱، ۶، ۳، ۴]. رمزنگاری بصری اجازه می‌دهد که اطلاعات بصری با سیستم بینایی انسان، بدون الگوریتم‌های رمزنگاری پیچیده، رمز شود [۵،۶] و یک روش اشتراک‌گذاری مخفی برای تصاویر است [۴] و برای نگرانی‌های امنیتی تضمین می‌نماید که هکرها هیچ سرنخی در مورد تصویر محرمانه[4] نمی توانند بدست آورند [۷].

در طرح اشتراک‌گذاری مخفیn از n, تصویر سیاه و سفید به n بخش تقسیم و بین n شرکت‌کننده توزیع می‌شود[۱۰، ۹، ۸]، که در صورت انباشتن[5] n بخش، تصویر محرمانه بازیابی می‌شود، این پدیده به عنوان طرح رمزنگاری بصری شناخته شده است [۱۱،۱۲،۱۳]، سپس آن را به اشتراک‌گذاری مخفیk از n[6] گسترش می‌دهند که n بخش از تصویر ایجاد می‌کنند و هر یک از

1 .Visual Cryptography
2 .Shamir
3 .Naor

4 .Secret Image
5 .Superimposed
6 .k-out-of-n secret sharing, (k,n)

نویسندهٔ عهده‌دار مکاتبات: نغمه محمدیnmohamadi@mail.kntu.ac.ir

آن‌ها را به n کاربر می‌دهند، با k تا از این بخش‌ها و روی هم انباشتن آن‌ها تصویر قابل دیدن و شناسایی است، اما با k-1 بخش هیچ اطلاعاتی درباره تصویر بدست نخواهد آمد [۱۴].

این مقاله به صورت زیر سازماندهی شده است:

در بخش ۲ کارهای مرتبط از قبیل تکنولوژی هالفتون[۷]، انواع روش‌های رمزنگاری بصری برای تصاویر سطح خاکستری و رنگی را شرح می‌دهیم. در بخش ۳ به معرفی روش‌های پیشنهادی می‌پردازیم و در بخش ۴ ارزیابی و مقایسه‌ای از این روش‌ها به عمل می‌آوریم و در بخش ۵ نتیجه‌گیری را ارائه می‌دهیم.

کارهای مرتبط

۱-تکنولوژی هالفتون

یک راه برای نمایش سطح خاکستری استفاده از تراکم نقاط چاپ شده است. به عنوان مثال، نقاط چاپ شده در بخش روشن، پراکنده و در بخش تاریک به صورت متراکم هستند (شکل ۱). این روش که از تراکم نقاط برای شبیه سازی سطح خاکستری استفاده می‌کند، هالفتون نام دارد و تصویر سطح خاکستری را به یک تصویر باینری قبل از پردازش تبدیل می‌کند.

برای مثال به تصویر سطح خاکستری در شکل ۲(الف) نگاه کنید. هر پیکسل در تصویر هالفتون (شکل۲(ب)) تنها دارای دو سطح رنگ (سیاه و سفید) است. از آنجا که چشم انسان نقاط چاپ شده خیلی کوچک را نمی‌تواند تشخیص دهد، در هنگام مشاهده یک نقطه، تمایل دارد که نقاط نزدیک آن را نیز تحت پوشش قرار دهد. ما می‌توانیم سطوح خاکستری مختلف را با وجود اینکه تصویر تبدیل شده فقط دارای دو رنگ سیاه و سفید است، با تراکم نقاط چاپ شده شبیه‌سازی کنیم [۷].

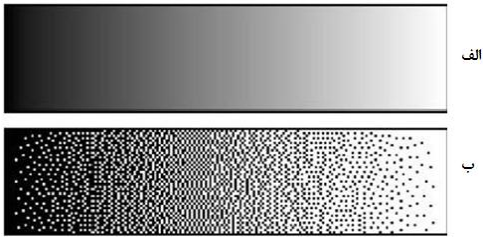
روش هالفتون به عنوان روش مبهم نمایی[۸] شناخته شده است و برای تبدیل تصویر سطح خاکستری به تصویر باینری استفاده می‌شود. این رویکرد به تصویر باینری اجازه می‌دهد که طرح رمزنگاری بصری[۹] را اجرا نماید. انواع مختلفی از الگوریتم‌های تکنیک هالفتون وجود دارد. یکی از تکنیک‌های شناخته‌شده تحت عنوان ماتریس مبهم‌نمایی است. این روش از مقدار مشخصی پیکسل سیاه و سفید در الگوها استفاده می‌کند تا مقیاس خاکستری بدست آید. درصد سیاه و سفید متفاوت، خاکستری‌های مختلفی را نشان می‌دهد (شکل۳). فرآیند هالفتون ، پیکسل‌های سطح خاکستری تصویر اصلی را به پیکسل‌های سیاه و سفید بر اساس الگو، نگاشت می‌کند [۱۱].

۲- طرح‌های رمزنگاری بصری

انواع مختلفی از طرح‌های رمزنگاری بصری وجود دارد، به عنوان مثال، طرح k از n می‌گوید که برای به رمز درآوردن یک تصویر، n بخش تولید می‌شود و برای رمزگشایی تصویر باید k بخش روی هم انباشته شوند، اگر تعداد بخش‌های انباشته شده کم‌تر از k باشد، تصویر اصلی مشخص نخواهد شد. طرح‌های دیگر رمزنگاری بصری، ۲ از n و n از n است. در طرح ۲ از n، برای رمزنگاری تصویر، n بخش تولید می‌شود و برای رمزگشایی، دو بخش روی هم انباشته می‌شود. در طرح n از n برای رمزگذاری تصویر، n بخش تولید می‌شود و برای رمزگشایی تصویر، n بخش باید روی هم انباشته شوند، اگر تعداد بخش‌های انباشته شده کم‌تر از n باشد، تصویر اصلی مشخص نخواهد شد. افزایش بخش‌ها و شرکت‌کنندگان به طور خودکار امنیت پیام رمزشده را افزایش می‌دهد [۲].

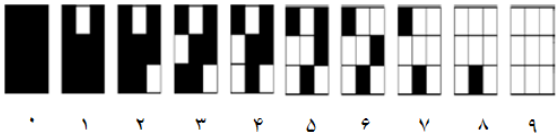
ایدهٔ اولیه از رمزنگاری بصری را می‌توانیم با توجّه به طرح رمزنگاری بصری ۲ از ۲ توضیح دهیم [۱]. تصویر باینری محرمانه S را در نظر بگیرید. دو بخش S_1 و S_2 (تصاویر باینری) که شامل دقیقاً دو زیر پیکسل به ازای هر پیکسل از تصویر محرمانه است، در شکل ۴ نشان داده شده است. اگر پیکسل S سیاه باشد، بصورت تصادفی یکی از دو ردیف اول شکل ۴ انتخاب می‌شود و بطور مشابه اگر پیکسل S سفید باشد، بصورت تصادفی یکی از دو ردیف آخر شکل ۴ انتخاب می‌شود.

7 .Halftone
8 .Dithering
9 .Visual Cryptography Schema,VCS



شکل۱: الف) تصویر با رنگ پیوسته ب) هالفتون

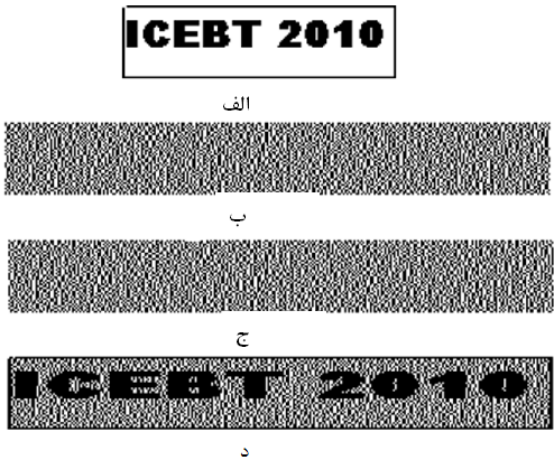
شکل۲: الف) تصویر با رنگ پیوسته ب) تصویر هالفتون



شکل۳: الگوی هالفتون ماتریس لرزشی با ۰-۹ سطح خاکستری

رنگ پیکسل	پیکسل اصلی	بخش s_1	بخش s_2	بخش s_1 + بخش s_2
سیاه	■	■□	□■	■■
سیاه	■	□■	■□	■■
سفید	□	■□	■□	■□
سفید	□	□■	□■	□■

شکل۴: الگو پیکسل‌ها برای رمزنگاری بصری ۲ از ۲ با ۲ زیر پیکسل



شکل۵: طرح رمزنگاری بصری ۲ از ۲ با دو زیر پیکسل بر هر پیکسل الف) تصویر اصلی ب) بخش اول ج) بخش دوم د) انطباق بخش اول و دوم بر هم

دو بخش s_1 و s_2 دارای تعداد برابری پیکسل سیاه و سفید است، بنابراین بازرسی یک بخش به تنهایی مشخص نمی‌کند که پیکسل اصلی سیاه یا سفید بوده است، این روش امنیت کاملی را فراهم می‌کند. مسئله‌ای که برای این طرح مطرح است این است که برای هر پیکسل از تصویر اصلی دو زیر پیکسل کدگذاری می‌شود و هر بخش در مد عمودی یا افقی (در اینجا افقی) قرار می‌گیرد. اگر اندازه تصویر اصلی s*s باشد اندازه بخش‌ها s*۲s خواهد، از این رو اعوجاج رخ می‌دهد (شکل ۵).

برای جلوگیری از اعوجاج افقی یا عمودی ما می‌توانیم از طرح لایه‌های ۴ زیر پیکسلی به جای ۲ زیر پیکسلی استفاده کنیم. در این حالت بخش‌ها دارای اندازه ۲s*2s و تصویر اصلی دارای اندازه s*s است و پیکسل‌ها بصورت یکنواخت گسترش یافته‌اند و اعوجاج به وجود نیامده‌است [۲]. در این حالت هر پیکسل در تصویر محرمانه به یک بلوک ۲*۲ در دو بخش با توجّه به قوانین موجود در شکل ۶ تجزیه می‌شوند. هنگامی که پیکسل سفید است، یکی از این دو ترکیب را در شکل ۶ برای تشکیل محتوای بلوک در دو بخش انتخاب می‌کنند و به همین ترتیب برای پیکسل سیاه این کار را انجام می‌دهند. بنابراین هنـگام انباشتن دو بخـش، بلـوک‌های متـناظر با پیکسل سیاه در تصویر محرمانه کاملاً سیاه دیده می‌شوند و آن‌هایی که مربوط به پیکسل سفیداند، نصف سفید و نصف سیاه‌اند که می‌توانند به عنوان پیکسل ۵۰٪ خاکستری دیده شوند. هنگام انباشته شدن سیاه با سیاه، سیاه؛ سیاه با سفید، سیاه و سفید با سفید، سفید نتیجه می‌شود [۷].

برای نمایش ریاضی طرح، هر پیکسل در تصویر ورودی (محرمانه) را به یک گروه زیر پیکسلِ b گسترش می‌دهیم، سپس به سفید مقدار صفر و به سیاه مقدار یک اختصاص می‌دهیم، برای این کار دو مجموعه ماتریسِ بولین c_0 و c_1 را مشخص می‌کنیم که باید بصورت سیستماتیک انتخاب شوند. هر ردیف از ماتریس در c_0 و c_1 ارزش یک گروه زیر پیکسل b در یک بخش را نشان می‌دهد. برای اشتراک‌گذاری یک پیکسل سفید (سیاه) در تصویر محرمانه، یکی از ماتریس‌های مجموعه c_0 (c_1)، به صورت تصادفی انتخاب می‌شوند، n ردیف از هر ماتریس بین n شرکت‌کننده توزیع می‌شود و هر یک، یک ردیف را دریافت می‌کنند. برای روشن شدن چگونگی استفاده از طرح رمزنگاری بصری آستانهٔ k از n (k,n) ، ما آستانهٔ (۲،۲) را در مثال زیر نشان می‌دهیم. ابتدا دو ماتریس تعریف می‌کنیم:

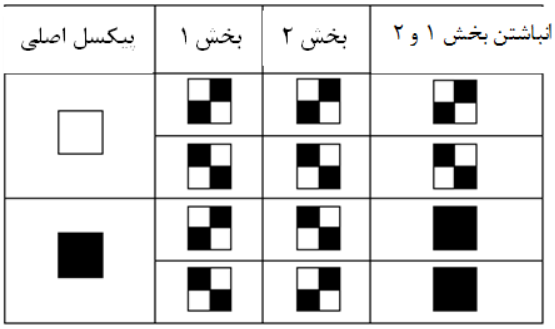
$$\mathbf{A_0} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}, \boldsymbol{A_1} = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

سپس دو مجموعه c_0 و c_1 ذکر شده در بالا را تعریف می‌کنیم:

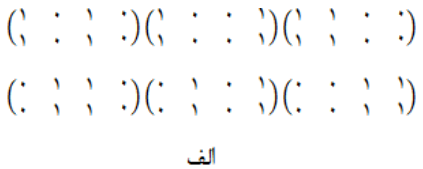
c_0 ={تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها A_0}

c_1 ={تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها A_1}

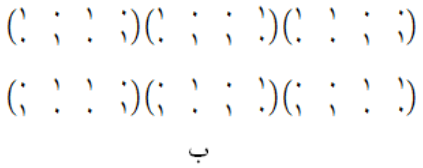
شکل ۷(الف) محتوای c_0 و شکل ۷(ب) محتوای c_1 را نشان می‌دهد.



شکل ۶: بخش‌بندی و روی هم انباشتن پیکسل‌های سیاه و سفید

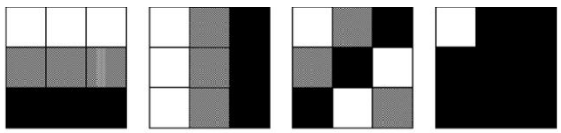


الف

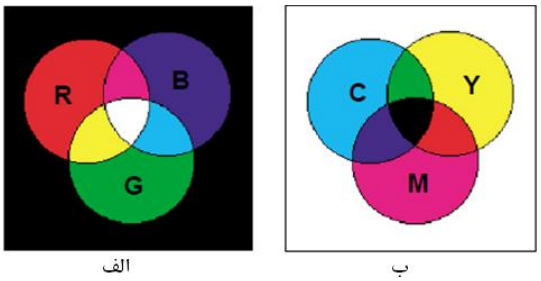


ب

شکل۷: c_0 و c_1 از رمزنگاری آستانه ۲ از ۲ الف) ماتریس‌های حاصل از جایگشت $\mathbf{A_0}$ در $\mathbf{c_0}$ ب) ماتریس‌های حاصل از جایگشت $\mathbf{A_1}$ در $\mathbf{c_1}$



شکل ۸: طرح رمزنگاری بصری (۳،۳) برای سطح خاکستری صفر الف) بخش۱ ب) بخش۲ ج) بخش۳ د) نتیجه انباشتن سه بخش



الف ب

شکل۹: الف) مدل افزایشی ب) مدل کاهشی

با انجام جایگشت، الگوهای بیش‌تری برای ردیف‌ها ایجاد می‌شود که همه با احتمال مساوی ظاهر می‌شوند و این اثر مانع ایجاد نظمی می‌شود که توسط مداخله‌گر کشف شود. پیکسل سفید بصورت دو زیر پیکسل سیاه و دو زیر پیکسل سفید رمزگشایی می‌شود و پیکسل سیاه بصورت چهار زیر پیکسل سیاه رمزگشایی می‌شود. برای به رمز درآوردن یک پیکسل سفید در تصویر اصلی، بخش اول را از ردیف اول ماتریس R_0 که به صورت تصادفی از c_0 انتخاب شده است و بخش دوم را از ردیف دوم R_0 بدست می‌آوریم. به همین ترتیب R_1 را بصورت تصادفی در c_1 برای به رمز درآوردن پیکسل سیاه انتخاب می‌کنیم.

در مورد بعدی ما یک نمونه از رمزنگاری بصری آستانهٔ (۴،۲) را نشان می‌دهیم که c_0 و c_1 به صورت زیر اند:

$c_0=\{$تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها $A_0\}$

$c_1=\{$تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها $A_1\}$

که A_0 و A_1 به صورت زیر است:

$$\mathbf{A_0}=\begin{pmatrix}\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\end{pmatrix},$$

$$\boldsymbol{A_1}=\begin{pmatrix}\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\ \mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}\\ \mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{1}\end{pmatrix}$$

ماتریس R_i به صورت تصادفی از مجموعه‌های c_0 و c_1 انتخاب می‌شود و هر بخش یکی از ردیف‌های این ماتریس را انتخاب می‌کند. در هر ردیف ماتریس R_i یک زیر پیکسل سیاه و سه زیر پیکسل سفید وجود دارد، بنابراین نتیجهٔ انباشتن دو بخش از پیکسل سفید، شامل یک زیر پیکسل سیاه و سه زیر پیکسل سفید است، درحالی که نتیجهٔ انباشتن دو بخش از پیکسل سیاه شامل دو زیر پیکسل سیاه و دو زیر پیکسل سفید است. زمانی که تعداد بخش‌ها بیش‌تر شود، تفاوت بین زیر پیکسل‌ها، واضح‌تر می‌شود [۱۵].

۳-رمزنگاری بصری برای سطوح خاکستری

مباحث در مورد رمزنگاری بصری برای سطوح خاکستری به ندرت مورد بحث قرار گرفته است، ورهول[10] و ون تلبورگ[11] (۱۹۹۷) روشی عمومی برای رمزنگاری بصری آستانهٔ (k,n) برای سطوح خاکستری را توضیح داده‌اند. برای یک تصویر با c سطح‌خاکستری ابتدا زیر پیکسل‌های b را گسترش می‌دهیم. هر زیر پیکسل ممکن است یکی از سطوح خاکستری (۰،۱،...c-۱) را بگیرد. بعد از این که همهٔ بخش‌ها انباشته شدند، اگر زیر پیکسل‌های متناظر با همهٔ بخش‌ها، سطح i خاکستری باشد، سطح i خاکستری نمایش داده می‌شود، در غیر این صورت سطح سیاه نمایش داده می‌شود. به عنوان مثال طرح آستانهٔ (۳،۳) را توضیح می‌دهیم. اگر سه سطح خاکستری وجود داشته باشد ما سه مجموعه ماتریس متعلق به سطوح خاکستری ۰،۱و۲ را نشان می‌دهیم:

$c_0=\{$تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها A_0

10 .Verheul
11 .Van tilborg

{تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها A_1 c_1={

{تمام ماتریس‌های بدست آمده از جایگشت ستون‌ها A_2 c_2={

A_0، A_1 و A_2 برابر است با:

$$A_0=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\0&1&2&1&2&0&2&0&1\end{pmatrix},$$
$$A_1=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\2&0&1&0&1&2&1&2&0\end{pmatrix},$$
$$A_2=\begin{pmatrix}0&0&0&1&1&1&2&2&2\\0&1&2&0&1&2&0&1&2\\1&2&0&2&0&1&0&1&2\end{pmatrix}$$

برای به رمز درآوردن یک پیکسل خاکستری در سطح صفر، بخش ۱ را از ردیف اول ماتریس .R که به صورت تصادفی از C۰ انتخاب شده است بدست می‌آوریم، بخش ۲ را از ردیف دوم ماتریس .R و بخش سوم را از ردیف سوم .R بدست می‌آوریم. الگوی بصری بخش‌ها و نتیجهٔ انباشتن آن‌ها در شکل ۸ نشان داده شده است، نتیجهٔ انباشته شدن زیرپیکسل‌های سه بخش در سمت بالا –چپ برابر با سطح صفر خاکستری تصویر اصلی است و بقیهٔ پیکسل‌ها، سیاه نمایش داده شده‌اند [۱۵].

البته برای تبدیل تصویر خاکستری به تصویر باینری در این بخش از الگوریتمی تحت عنوان SFCOD (مبهم‌نمایی مرتب شده منحنی فضای پر شده)[۱۲] استفاده شده است و سپس از طرح رمزنگار بصری استفاده می‌شود، اندازهٔ تصویر در این روش کم‌تر از روش پیشنهادی ورهول و ون تلبورگ افزایش می‌یابد [۱۵].

۱-۳ ساختار طرح رمزنگاری بصری توسعه یافته برای اشتراک‌گذاری مخفی

به وسیله جاسازی بخش‌های تصادفی نتیجه شده از طرح رمزنگاری بصری، در داخل تصویر پوشش[۱۳] ساختار EVCS (رمزنگاری بصری توسعه یافته)[۱۴] ایجاد می‌شود. EVCS چیزی شبیه به نهان‌نگاری[۱۵] است که در آن بخش‌هایی در داخل تصاویر پوششِ معنادار جاسازی می‌شوند و به این ترتیب مردم هیچ گونه شکی بر وجود بخش‌ها در داخل این تصاویر نخواهند برد. برای بازیابی تصویر اصلی زیر مجموعه‌ای از تصاویر پوششی روی هم انباشته می‌شوند [۱۱].

۴-رمزنگاری بصری برای تصاویر رنگی

۱-۴- اصول اساسی رنگ‌ها

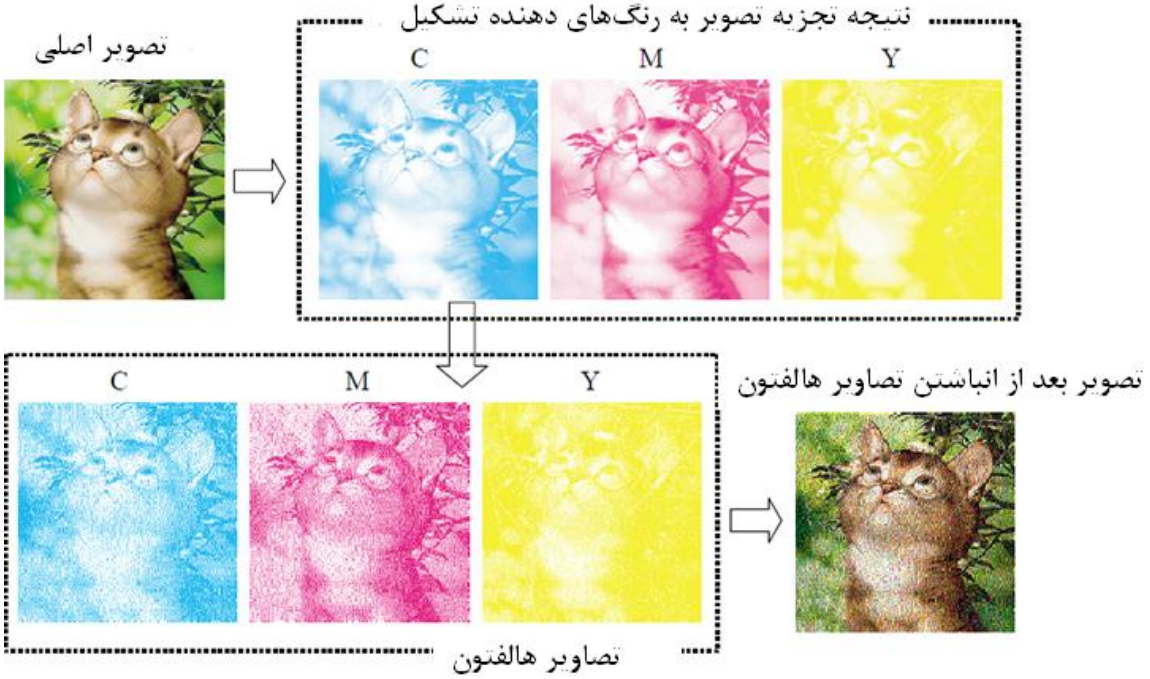
دو نوع مدل برای رنگ‌ها معرفی شده است: مدل افزایشی[۱۶] و مدل کاهشی[۱۷] (شکل۹).

مدل افزایشی شامل قرمز، سبز، آبی[۱۸](RGB) است. رنگ‌های مختلف با ترکیب این سه رنگ ایجاد می‌شود. هنگامی این سه رنگ به یک شدّت باهم ترکیب شوند، سفید را ایجاد می‌کند. روشنایی رنگ بدست آمده از ترکیب، از رنگ‌های شرکت‌کننده در ترکیب بیش‌تر است، مانیتور کامپیوتر مثالی از مدل افزایشی است.

مدل کاهشی رنگ بوسیله ترکیبی از رنگ‌های منعکس شده از اجسام نشان داده می‌شود (نگاه به سیب در نور طبیعی). با مخلوط شدن رنگ‌های فیروزه‌ای، سرخابی، زرد (CMY) طیف وسیعی از رنگ‌ها ایجاد می‌شود. رنگ‌هایی که با هم ترکیب می‌شوند، شدّت نور را کاهش می‌دهند, در نتیجه تاریک‌تر می‌شوند، به همین دلیل مدل کاهشی نامیده می‌شود. چاپگرها مثالی از این مدل‌اند. در رویکرد رجمن[۱۹] و پرینل[۲۰] بلوک‌ها با رنگ‌های قرمز و سبز و آبی و سفید (شفاف) پر می‌شوند که مناسب نیست. در مدل افزایشی هر رنگ که با سفید مخلوط شود، سفید می شود، بنابراین معقول‌تر است که از سیاه به جای سفید استفاده شود. از سوی دیگر در مدل کاهشی ترکیب هر دو رنگ قرمز، سبز و آبی، سیاه را نتیجه می‌دهد و قرمز، سبز، آبی در ترکیب با سیاه تغییر نمی‌کنند. بنابراین بهتر است بلوک‌ها را با فیروزه‌ای، سرخابی و زرد، سفید پر کنیم.

12 .Space-Fillingcurve Ordered Dithering
13 .Cover Image
14 .Extended Visual Cryptography Scheme

15 .Steganography
16 .Additive Model
17 .Subtractive Model
18 .Red,Green,Blue
19 .Rijman
20 . Preneel



شکل ۱۰: تبدیل تصویر رنگی به تصاویر هالفتون

در سیستم رنگ واقعی، قرمز، سبز و آبی با ۸ بیت نمایش داده می‌شوند، پس هر کدام از تک رنگ‌ها از ۰- ۲۵۵ تغییر می‌کنند. وقتی (R,G,B) نمایندهٔ یک پیکسل رنگی باشد، (0,0,0) نشان دهنده سیاه و (255,255,255) نشان دهنده سفید است. در رمزنگاری بصری، ما از CMY برای چاپ رنگ‌ها بر روی بخش‌ها استفاده می‌کنیم. از آنجا که مدل افزایشی مکمّل مدل کاهشی است بنابراین اگر (C,M,Y) نمایندهٔ یک پیکسل باشد، (0,0,0) نشان دهنده کامل سفید و (255,255,255) کامل سیاه است.

از آنجا که چاپگرها از جوهر C,M,Y برای نمایش رنگ‌ها استفاده می‌کنند، بنابراین یک تصویر رنگی را قبل از پرینت به سه بخش رنگی جداگانه C,M,Y تجزیه می‌کنند. این سه بخش از سه تصویر تک رنگ ساخته شده‌اند .از آنجا که جوهرِ رنگ گران است و برای تشکیل رنگ سیاه هر سه رنگ باید چاپ شوند، بنابراین چاپگر جوهر سیاه را هنگام چاپ استفاده می‌کند، بنابراین چهار بخش تصویر جداگانه ایجاد می‌کند. این تصاویر مانند تصویر سطح خاکستری‌اند که هر پیکسل سطح رنگی خود را دارد و قبل از چاپ به یک تصویر هالفتون تبدیل می‌شود. سه تصویر هالفتون عبارت است از فیروزه‌ای – سفید، سرخابی- سفید و زرد- سفید. پس از انباشتن این تصاویر, همه نوع رنگ در تصویر اصلی نمایش داده می‌شود (شکل ۱۰). هر پیکسل P_{ij} از تصویر رنگی P از ترکیب متناظر C_{ij}، M_{ij}، Y_{ij} در سه تصویر هالفتون Y,M,C بدست می‌آید. برای هر پیکسل C_{ij}، M_{ij}، Y_{ij} دو مقدار خالی یا پر وجود دارد. که ۰ بیان‌گر خالی و ۱ نشان‌گر رنگ مربوطه است. بنابراین P_{ij} دارای ترکیبات زیر است:

(0,0,0) , (1,0,0) , (0,1,0) , (0,0,1) , (1,1,0)
(0,1,1) , (1,0,1) ,(1,1,1)

که در آن (0,0,0) نشان‌دهنده سفید و (1,1,1) نشان دهنده سیاه است. از آنجا که C,M,Y رنگ‌های اصلی‌اند، ویژگی‌های معمولی را حفظ می‌کنند، بنابراین C(Y یا M) به علاوه C(Y یا M) برابر C(Y یا M) و C(Y یا M) به علاوه سفید برابر C(Y,M) و سفید به علاوه سفید برابر سفید است [۷].

۲-۴-روش‌های رمزنگاری بصری تصاویر رنگی

در این بخش به توضیح سه روش رمزنگاری تصاویر رنگی می‌پردازیم [۷].

روش۱: از روش نشان داده شده در شکل ۱۰ برای تبدیل تصویر محرمانه به تصاویر هالفتون C,M,Y استفاده می‌کنیم، سپس هر پیکسل از تصاویر هالفتون را

به بلوک‌های ۲*۲ که به یک رنگ هستند، با توجّه به مدل ارائه شده در شکل۶ گسترش می‌دهیم. هر بلوک در بخش‌های رنگی، شامل دو پیکسل سفید و دو پیکسل رنگی است. علاوه بر این ما از ماسک سیاه و سفید برای جلوگیری از ایجاد رنگ‌های غیر منتظره در تصویر انباشته شده استفاده می‌کنیم ، بطوری که تنها رنگ‌های مورد انتظار ایجاد شوند (شکل ۱۱). اگر پیکسل P_{ij} از تصویر رنگی (0,0,0) باشد، توزیع پیکسل‌ها در بخش‌ها به صورت سطر اولِ شکل ۱۱ نشان داده می‌شود. پس از انباشته شدن بخش‌ها، تمام پیکسل‌های رنگی بر روی بخش‌ها توسط پیکسل سیاه پوشیده می‌شود و فقط پیکسل سفید نشان داده می‌شود، در نتیجه نشان دهنده رنگ سفید است. علاوه بر این می‌توانیم توزیع تصویر انباشته شده را از لحاظ کمّیّت رنگ‌ها آنالیز کنیم. برای نمونه ردیف پنجم شکل ۱۱ را در نظر بگیرد، C,M نشان داده می‌شود و Y با رنگ سیاه پوشیده می‌شود. از آنجا که سیاه به عنوان ترکیب C,Y,M دیده می‌شود و C,M در هر چهار خانه بلوک ۲*۲ و زرد در دو خانه دیده می‌شود، بنابراین شدّت رنگ(C,M,Y) برابر با (1,1,1/2) است.

الگوریتم روش اول بصورت زیر است:

۱-تبدیل تصویر رنگی به سه تصویر هالفتون Y,M,C.

۲-برای هر پیکسل P_{ij} با اجزای Y_{ij}،M_{ij}،C_{ij} از تصویر P موارد زیر را انجام دهید:

الف) یک ماسک سیاه و سفید با سایز ۲*۲ انتخاب می‌شود و به دو خانه از آن رنگ سیاه و به سایر مواضع رنگ سفید اختصاص داده می‌شود.

ب) پس از انتخاب ماسک، موقعیت پیکسل‌های فیروزه‌ای در بلوک مربوط به بخش فیروزه‌ای را تعیین می‌کنیم. این با توجّه به موقعیت پیکسل‌های سیاه در ماسک و C_{ij} انجام می‌شود.

کمیت رنگ‌ها(C,M,Y)	نتیجه انباشتن	بخش۳ (Y)	بخش۲ (M)	بخش۱ (C)	مقدار (C,M,Y)	ماسک
(۱/۲،۱/۲،۱/۲)					(۰،۰،۰)	
(۱،۱/۲،۱/۲)					(۱،۰،۰)	
(۱/۲،۱،۱/۲)					(۰،۱،۰)	
(۱/۲،۱/۲،۱)					(۰،۰،۱)	
(۱،۱،۱/۲)					(۱،۱،۰)	
(۱/۲،۱،۱)					(۰،۱،۱)	
(۱،۱/۲،۱)					(۱،۰،۱)	
(۱،۱،۱)					(۱،۱،۱)	

شکل۱۱: روش ۱ از رمزنگاری بصری

شکل۱۲: چهار بخش و نتیجه انباشتن آنها الف)بخش۱ ب)بخش۲ ج) بخش۳ د) ماسک ه) نتیجه انباشتن بخش‌ها

کمیت رنگ‌ها (C.M.Y)	نتیجه حاصل	روش	نتیجه انباشتن	بخش۲	بخش۱	مقدار (C,M,Y)
(۱/۴،۱/۴،۱/۴)		جایگشت یکسان بخش۱ و بخش۲				(۰،۰،۰)
(۱/۲،۱/۴،۱/۴)		جا به جایی فیروزه‌ای و سفید				(۱،۰،۰)
(۱/۴،۱/۲،۱/۴)		جا به جایی سرخابی و سفید				(۰،۱،۰)
(۱/۴،۱/۴،۱/۲)		جا به جایی زرد و سفید				(۰،۰،۱)
(۱/۲،۱/۲،۱/۴)		جا به جایی فیروزه‌ای و سرخابی				(۱،۱،۰)
(۱/۴،۱/۲،۱/۲)		جا به جایی زرد و سرخابی				(۰،۱،۱)
(۱/۲،۱/۴،۱/۲)		جا به جایی فیروزه‌ای و زرد				(۱،۰،۱)
(۱/۲،۱/۲،۱/۲)		جا به جایی دو جفت				(۱،۱،۱)

شکل ۱۳:رمزنگاری بصری روش ۲

اگر $C_{ij}=1$ (جزء فیروزه‌ای آشکار است) باشد، مواضع متناظر با پیکسل سفید در ماسک با پیکسل فیروزه‌ای پر می‌شود و بقیهٔ مواضع خالی می‌مانند. اگر $C_{ij}=0$ (جزء فیروزه‌ای پنهان است) باشد، رنگ‌ها به روش بر عکس در بالا پر می‌شوند و مواضع متناظر با پیکسل سیاه در ماسک با پیکسل فیروزه‌ای پر می‌شود و بقیهٔ مواضع خالی می‌مانند. سرانجام بلوک را به موقعیت بخش ۱ اضافه می‌کنیم.

ج) براساس مرحله "ب" موقعیت پیکسل‌های سرخابی در بلوک بخش ۲ را با توجّه به ارزش M_{ij} و موقعیت پیکسل‌های سیاه در ماسک و موقعیت پیکسل‌های زرد در بلوک بخش ۳ را با توجّه به ارزش Y_{ij} و موقعیت پیکسل‌های سیاه در ماسک، تعیین می‌کنیم.

۳-تکرار مرحله ۲ تا زمانی که هر پیکسل از تصویر P تجزیه شود، از این رو ۴ بخش فیروزه‌ای، سرخابی، زرد، سیاه از رمزنگاری بصری برای بخش‌بندی تصویر محرمانه بدست می‌آید.

۴-پس از انباشتن بخش‌ها، تصویر محرمانه را می‌توان با چشم رمزگشایی کرد.

در شکل ۱۲ این روش استفاده شده است، چهار بخش ایجاد شده کاملاً بی نظم بوده است و نمی‌توان هیچ سر نخی از تصویر اصلی را به تنهایی نشان‌دهند. اگر چه قسمت سیاه در تصویر انباشته شده هنوز سیاه است و قسمت سفید دیگر سفید محض نیست و تا حدودی وضوح تصویر کاهش یافته‌است اما هنوز محتوای تصویر قابل شناسایی است. بدون انباشتن ماسک سیاه بر سه بخش دیگر، رنگ‌های غیر منتظره ایجاد می‌شود و با قسمت معنادار تصویر مخلوط می‌شود؛ در نتیجه محرمانگی تصویر دست نخورده باقی می‌ماند. بنابراین کنترل دو سطحیِ امنیت ایجاد می‌شود. به عنوان مثال تا زمانی که مدیر شرکت، ماسک سیاهِ تصویر محرمانه را نگه دارد و بقیه بخش‌ها را به زیر دستان دهد، محتوای تصویر، محرمانه باقی می‌ماند، حتی اگر تمام زیردستان برای سرقت اطلاعات مخفی توطئه کنند، بنابراین در این شرایط، ماسک سیاه را می‌توان به عنوان امضا مدیر در نظر گرفت.

روش ۲: هر پیکسل از تصویر هالفتون را به بلوک‌های ۲*۲ در دو بخش گسترش می‌دهیم, هر بلوک را با رنگ‌های فیروزه‌ای، سرخابی، زرد، سفید (شفاف) به ترتیب پر می‌کنیم. دو بخش انباشته شده، با استفاده از این چهار رنگ، می‌توانند با جایگشت، رنگ‌های مختلف را تولید کنند (شکل۱۳). توزیع رنگ‌ها در بخش ۱ و ۲ در سطر اول یکسان است و چشم انسان اثر این چهار پیکسل انباشته شده را متعادل می‌کند و به رنگ تقریباً سفید می‌بیند. از لحاظ شدّت، فیروزه‌ای و سرخابی و زرد ۱/۴ بلوک را اشغال کرده‌اند. در بخش ۱ و ۲ از سطر دوم، موقعیت‌های فیروزه‌ای و سفید، برای آشکار شدن دو پیکسل فیروزه‌ای جا به جا می‌شوند. بعد از انباشته شدن، یک پیکسل زرد و یک پیکسل سرخابی درون چهار خانه دیده می‌شود. بنابراین شدّت رنگ بصورت (۱/۴، ۱/۴، ۱/۲) است و به رنگ فیروزه‌ای بنظر می‌آید. مراحل کار بصورت الگوریتم زیر است:

۱)تصویر رنگی به سه تصویر هالفتون C,M,Y تبدیل می‌کنید.

۲)برای هر پیکسل P_{ij} از تصویر P، موارد زیر را انجام می‌دهید:

الف)یک بلوک ۲*۲ در بخش ۱ گسترش دهید و با رنگ‌های فیروزه‌ای، سرخابی, زرد و سفید بصورت تصادفی پر کنید.

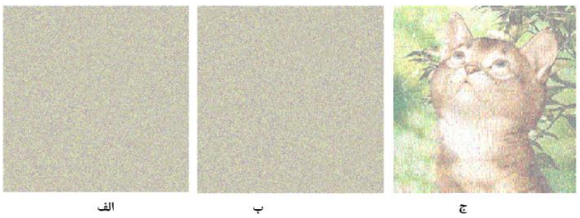
ب)بلوک ۲*۲ در بخش ۲ را بر اساس جایگشت چهار رنگ در بخش ۱ و ارزش C_{ij}،M_{ij}،Y_{ij} تولید کنید و توزیع رنگ در بلوک مربوطه را با توجّه به شکل ۱۳ تعیین کنید.

۳) مرحله ۲ را تا زمانی که تمام پیکسل‌های تصویر P تجزیه شوند ادامه می‌دهید. از این رو برای بخش‌بندی تصویر محرمانه، دو بخش بدست می‌آید.

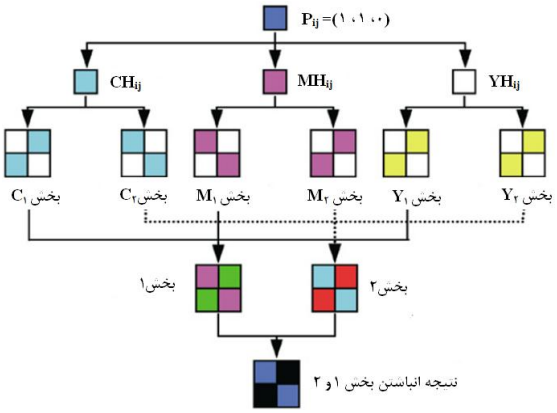
۴)پس از انباشته شدن دو بخش، تصویر محرمانه توسط چشم انسان قابل رمزگشایی است.

برای مثال شکل ۱۴ را ببینید. روش ۲ زحمت روش ۱ را کاهش داده است و تنها دو بخش برای رمزگذاری تصویر محرمانه ایجاد می‌کند، بنابراین دو بخش

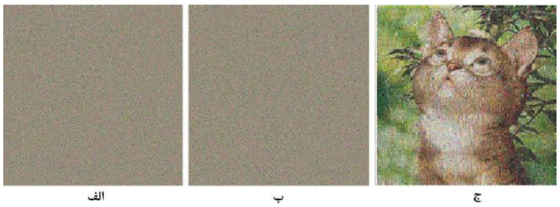
دارای امتـیاز برابراند، از این‌رو کنـترل دو سـطحی مانند روش ۱ را ندارد. شدّت رنگ در روش ۱ بین (۱/۲، ۱/۲، ۱/۲) و (۱،۱،۱) است و در روش ۲ بین (۱/۴، ۱/۴، ۱/۴) و (۱/۲، ۱/۲، ۱/۲) اسـت, به عبـارتی پـس از انبـاشـتن بخش‌ها در روش ۲ وضوح تصویر ۲۵٪ تصویر اصلی است و در روش ۱، ۵۰٪ تصویر اصلی است و تصویر ایجاد شده توسط روش ۲ روشن‌تر از روش ۱ است ولی اگر تصویر اصلی به طور طبیعی تیره باشد روش ۲ بهتر عمل می‌کند.



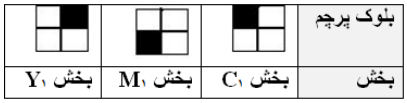
شکل۱۴: دو بخش و نتیجه انباشتن الف)بخش ۱ ب) بخش ۲



شکل۱۵: تجزیه پیکسل رنگی و بازیابی آن



شکل ۱۶: دو بخش ایجاد شده و انباشتن آنها الف) بخش۱ ب) بخش ۲



شکل ۱۷: الگوهای بلوک پرچم

روش ۳: این روش به منظور کاهش زحمت روش ۱ و از دست دادن وضوح در روش ۲ ایجاد شده است. این روش به دو بخش نیاز دارد و وضوح رمزنگاری بصری رنگی را بیش از حدّ قربانی نمی‌کند. تصویر محرمانه را به سه تصویر هالفتون C,M,Y تبدیل می‌کند و از تکنیک رمزنگاری سطح خاکستری شکل ۶ استفاده می‌کند و ۶ بخش موقت $C_1,C_2,M_1.M_2.Y_1,Y_2$ را تولید می‌کند، هر یک از بلوک‌های این بخش‌ها شامل دو پیکسل سفید و دو پیکسل رنگی است. در این روش C_1,M_1,Y_1 را برای تشکیل بخش۱ و C_2,M_2,Y_2 را برای تشکیل بخش ۲ ترکیب می‌کنند. برای هر بلوک در بخش ۱ و ۲ شدّت رنگ (۱/۲، ۱/۲، ۱/۲) است، یعنی پس از انباشتن دو بخش، محدودهٔ شدّت رنگ بین (۱/۲، ۱/۲، ۱/۲) و (۱،۱،۱) است (شکل ۱۶). الگوریتم این روش بصورت زیر است:

۱) تصویر را به سه تصویر هالفتون C,M,Y تبدیل می‌کنیم.

۲) برای هر پیکسل P_{ij} از تصویر P، موارد زیر را انجام دهید:

الف) با توجّه به روش سنتی رمزنگاری بصری سیاه و سفید، Y_{ij}،M_{ij}،C_{ij} را به شش بلوک $C_{1ij},C_{2ij},M_{1ij},M_{2ij},Y_{1ij},Y_{2ij}$ گسترش دهید.

ب) بلوک‌های Y_{1ij},M_{1ij},C_{1ij} را با هم ترکیب کنید و بلوک متناظر با بخش ۱ را پر کنید.

ج) بلوک‌های Y_{2ij},M_{2ij},C_{2ij} را باهم ترکیب کنید و بلوک متناظر با بخش ۲ را پر کنید.

۳) مرحلهٔ ۲ را تا زمانی که هر پیکسل در تصویر P، تجزیه شود، ادامه دهید. از این رو دو بخش رمزنگاری بصری برای تصویر محرمانه بدست می‌آید.

۴) پس از انباشتن دو تصویر، تصویر رمزگذاری شده می‌تواند با چشم انسان رمزگشایی شود.

برای مثالی از این روش شکل ۱۶ را ببینید. این روش به دو بخش نیاز دارد، پس از روش ۱ بهتر است و از دست دادن وضوح تصویر کم‌تر است، پس از روش ۲ بهتر است. اما مانند روش ۲ دو بخش تولید می‌کند که امتیاز برابر دارد، پس کنترل امنیّت دو سطحی را ارائه نمی‌دهد

- **روش‌های پیشنهادی**

۱- روش پیشنهادی اول

این روش را برای رمزنگاری بصری تصاویر رنگی پیشنهاد می‌کنیم، قوانین آن طبق مدل کاهشی رنگ‌ها است. از روشِ نشان داده شده در شکل ۱۱ برای تبدیل تصویر محرمانه به تصاویر هالفتون C،M،Y استفاده می‌کنیم. سپس هر پیکسل از تصاویر هالفتون را به بلوک‌های ۲*۲ با توجّه به مدل ارائه شده در شکل ۶ گسترش می‌دهیم، به این صورت که هر پیکسل رنگی مانند پیکسل سیاه در این مدل عمل می‌نماید. هر بلوک شامل دو پیکسل رنگی و دو پیکسل سفید است. بعد از اعمال این مدل برای هر تصویر هالفتون Y،M،C دو بخش ایجاد می‌شود که به ترتیب$Y_۲$،$Y_۱$،$M_۲$،$M_۱$،$C_۲$،$C_۱$ است. پیکسل‌های رنگی مربوط به بخش $Y_۱$،$M_۱$،$C_۱$ به رنگ سیاه تغییر می‌کند و برای تشخیص رنگ مربوط به این بخش‌ها از بلوک پرچم استفاده می‌شود. در نهایت چهار بخش برای توزیع بین شرکت‌کنندگان ایجاد می‌شود.

الگوریتم این روش به شرح زیر است که فلوچارت آن در شکل ۱۸ نشان داده شده است:

مرحلهٔ۱: تصویر محرمانه (اصلی) را به سه تصویر هالفتون C,M,Y (فیروزه‌ای – سرخابی- زرد) با توجّه به روش ارائه شده در شکل ۱۱ تجزیه می‌نماییم،به این ترتیب که ابتدا تصویر به سه رنگ تشکیل دهنده خود شکسته می‌شود، سپس هر یک از این تصاویر ایجاد شده را با استفاده از الگوریتم هالفتون به تصاویر هالفتون که بصورت باینری هستند، تبدیل می‌نماییم. پس از انباشتن سه تصویر هالفتون ایجاد شده، تصویر باینری P ایجاد می‌شود که به هر پیکسل این تصویر، P_{ij} گفته می شود و به هر پیکسل تصویرهای هالفتون C,M,Y به ترتیبY_{ij},M_{ij},C_{ij} می‌گوییم.

مرحلهٔ۲: برای هر پیکسل P_{ij} از تصویر P عمل زیر را انجام می‌دهیم:

با توجّه به روش سنتی رمزنگاری بصری سیاه و سفید ۲ از ۲(شکل ۶ را ببینید)، پیکسل‌های Y_{ij},M_{ij},C_{ij} را به بلوک‌های ۲*۲ گسترش می‌دهیم، در واقع برای هر کدام از تصویرهای C,Y,M دو بخش ایجاد می‌کنیم:

$C \rightarrow C_1, C_2$
$M \rightarrow M_1, M_2$
$Y \rightarrow Y_1, Y_2$

مرحلهٔ۳: تا زمانی که همهٔ پیکسل‌ها در تصویر P، گسترش یابند، مرحلهٔ۲ را تکرار می‌کنیم. از این‌رو ۶ بخش $Y_2, Y_1, M_2, M_1, C_2, C_1$ برای تصویر محرمانه بدست می‌آید.

مرحلهٔ۴: پیکسل P_{ij} را به صورت تصادفی انتخاب و پیکسل‌های متناظر با آن‌ها را در C,M,Y پیدا می‌نماییم و بلوک متناظر با آن پیکسل‌ها را در ۳ بخش Y_1, M_1, C_1 با توجّه به الگو ارائه شده در شکل ۱۷ جایگزین می‌کنیم. این بلوک ها نقش پرچم[21] را دارند. لازم به ذکر است که، از پرچم در مرحلهٔ۶ برای تشخیص رنگ بخش‌ها، استفاده می‌شود.

مرحلهٔ۵: در این مرحله تمام پیکسل‌های موجود رنگی (غیر سفید) در ۳ بخش C_1 وM_1 وY_1 را به رنگ سیاه تغییر رنگ می‌دهیم و بقیهٔ پیکسل‌ها سفید باقی می‌مانند، این سه بخش جدید را C_1' ،M_1' وY_1' می‌نامیم و بخش C2,M2,Y2 را باهم ترکیب (انباشته) می‌نماییم و یک بخش جدید به نام B ایجاد می‌کنیم. Y1',M1',C1' و B را بین چهار شرکت‌کننده توزیع می‌نماییم و به هر یک، تنها یک بخش، می‌دهیم، وجود هر چهار بخش و البته بلوک پرچم برای رمزگشایی تصویر محرمانه لازم است.

مرحلهٔ۶: برای بدست آوردن تصویر محرمانه به این صورت عمل می‌نماییم، چهار شرکت‌کننده بخش‌های خود را ارائه می‌دهند، مکان بلوک پرچم در سه بخش سیاه و سفید موجود برای تعیین رنگ هر یک از این بخش‌ها، داده می‌شود و با توجّه به حالت پرچم در هر بخش، رنگ آن بخش تشخیص داده می‌شود و بخش‌های C1,M1,Y1 مشخص می‌شوند، پیکسل‌های سیاه به رنگ مربوط به بخشی که به آن تعلق داشته‌اند باز می‌گردند، به این صورت که اگر بلوک پرچم، نشان دهندهٔ بخش فیروزه‌ای باشد، تمام پیکسل‌های سیاه آن بخش به فیروزه‌ای، تغییر رنگ می‌دهند، پس از بازیابی رنگ هر بخش، بخش C1، M1 ، Y1 را با بخش B ترکیب (انباشته) می‌کنیم و تصویر محرمانه را بدست می‌آوریم.

موقعیت بلوک پرچم که به صورت تصادفی انتخاب می‌شود به همراه بخش B، اگر به مدیر داده شود، می‌تواند به عنوان امضاء مدیر در نظر گرفته شود؛ به این صورت که اگر زیردستان با هم توطئه کنند و بخواهند اطلاعات مخفی را سرقت کنند چون بخش مدیر و محل بلوک پرچم تصادفی را نمی‌دانند، نمی‌توانند تصویر محرمانه را بازیابند و در نتیجه کنترل دو سطحی ایجاد می‌نماید. در شکل ۱۹ این روش استفاده شده است.

۲- روش پیشنهادی دوم

این روش را برای رمزنگاری بصری تصاویر رنگی پیشنهاد نموده‌ایم که بسیار ساده است و مانند روش پیشنهادی اول، طبق مدل کاهشی رنگ‌ها است.

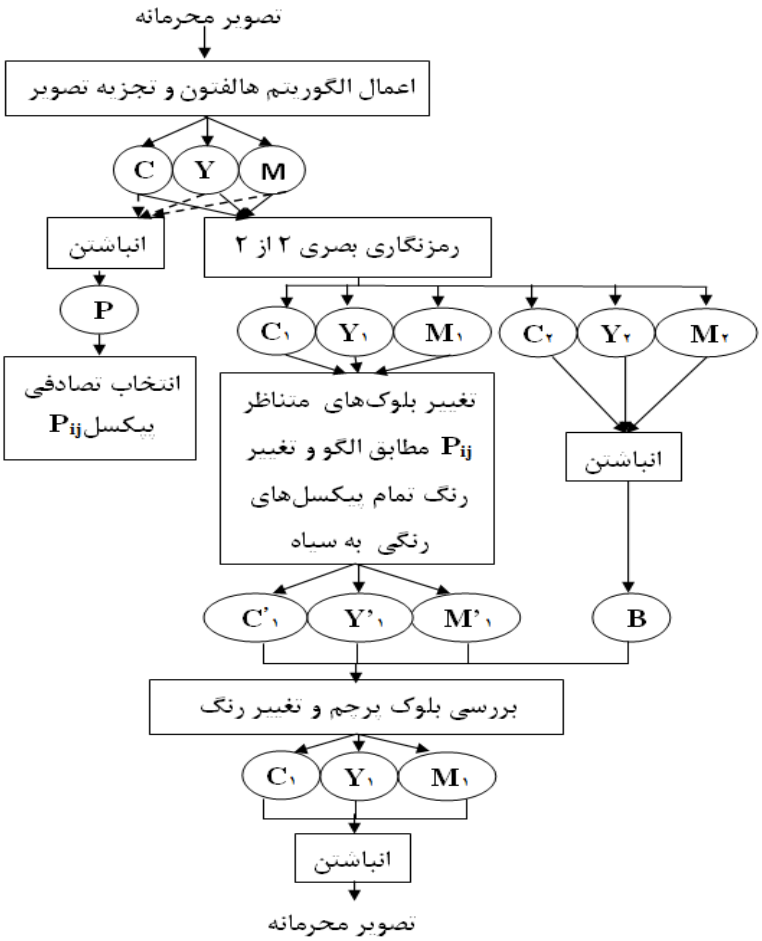
از روشِ نشان داده شده در شکل ۱۱ برای تبدیل تصویر محرمانه به تصاویر هالفتون C،M،Y استفاده می‌کنیم، سپس از سه تصویر هالفتون ایجاد شده، تنها از یکی برای ادامهٔ کار استفاده می‌نماییم و پیکسل‌های رنگی آن را به رنگ سیاه، تغییر می‌دهیم و هر پیکسل از این تصویر را طبق مدل ارائه شده در شکل ۶ گسترش می‌دهیم و دو بخش ایجاد می‌نماییم. برای رمزگشایی تصویر محرمانه حضور هر دو بخش لازم است. نتیجهٔ رمزگشایی این روش، تصویری سیاه و سفید با وضوح پایین است.

الگوریتم این روش به شرح زیر است که فلوچارت آن در شکل ۲۰ نشان داده شده است:

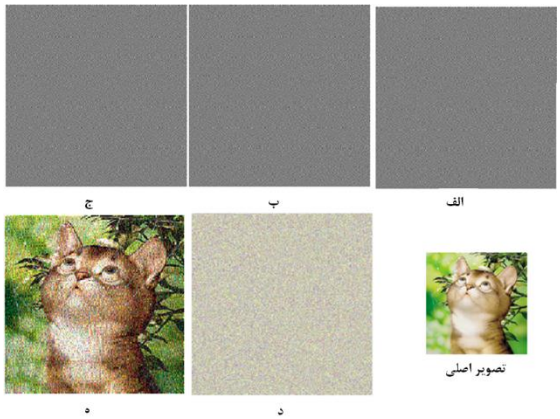
مرحلهٔ۱: تصویر محرمانه (اصلی) را با توجّه به روشی که در شکل ۱۱ ارائه شده است به سه تصویر هالفتون C,M,Y تبدیل می‌کنیم.

مرحلهٔ۲: یکی از سه تصویر هالفتون ایجاد شده (C,M,Y) را با توجّه به این که کدام یک پیکسل رنگی بیش‌تری نسبت به دیگر تصویرها دارد را انتخاب می‌کنیم، با این کار تصویر رمزگشایی شده بیش‌تر قابل درک می‌شود. برای نمونه، تصویر M را انتخاب نموده‌ایم.

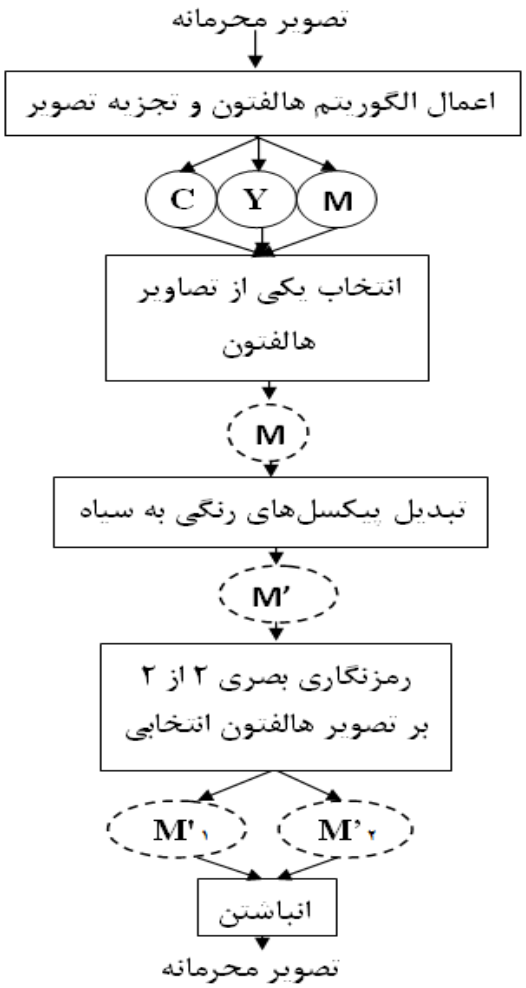
21. Flag



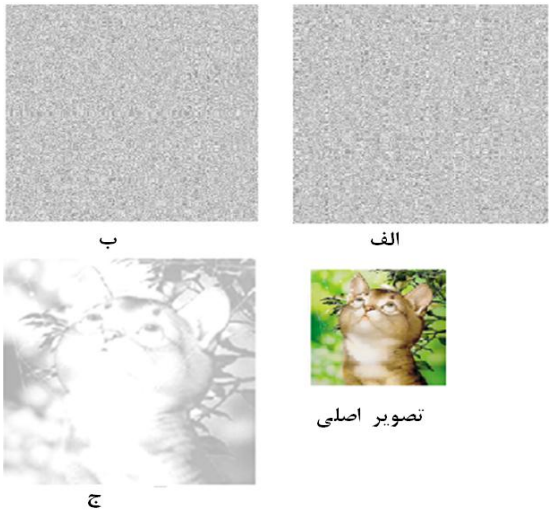
شکل ۱۸: فلوچارت روش پیشنهادی اول



شکل ۱۹: چهار بخش ایجاد شده و نتیجه انباشتن آنها الف) بخش C'۱ ب) بخش Y'۱ ج) بخش M'۱ د)بخش B ه) نتیجه انباشتن بخش‌ها



شکل ۲۰: فلوچارت روش پیشنهادی دوم



شکل ۲۱: دو بخش ایجاد شده و نتیجه انباشتن آنها
الف) بخش۱ ب) بخش۲ ج) نتیجه انباشتن بخش‌ها

مرحلهٔ۳: پیکسل‌های رنگی تصویر هالفتون انتخابی را به رنگ سیاه تغییر می‌دهیم و پیکسل‌های سفید بدون تغییر باقی می‌مانند.

مرحلهٔ۴: با استفاده از طرح رمزنگاری بصری سیاه و سفید ۲ از ۲ (شکل ۶) تصویر هالفتون انتخابی را به دو بخش ۱ و ۲ تقسیم می‌نماییم. بخش ۱ و ۲ را بین دو شرکت‌کننده توزیع می‌نماییم، به طوری که به هر شرکت‌کننده، تنها یک بخش می‌رسد، با داشتن تنها یک بخش هیچ اطلاعاتی دربارهٔ تصویر به دست نمی‌آوریم.

مرحلهٔ۵: برای بازیابی تصویر محرمانه، دو شرکت‌کننده بخش‌های خود را ارائه می‌دهند, سپس دو بخش ۱ و ۲ را با هم ترکیب (انباشته) می‌کنیم و تصویری سیاه و سفید از تصویر محرمانه، ایجاد می‌شود.

این روش بر خلاف روش اول کنترل دو سطحی ایجاد نمی‌کند و تصویر بازیابی شده وضوح کم‌تری نسبت به روش اول دارد. در شکل ۱۴ از این روش استفاده شده است.

- **ارزیابی و مقایسه**

در این قسمت به مقایسه و ارزیابی دو روش پیشنهادی ارائه شده در بخش قبل می‌پردازیم. همان طور که در جدول ۱ نشان داده شده است، این دو روش از نظر تعداد بخش‌های ایجاد شده، روش رمزنگاری، اندازهٔ تصویر بازیابی شده و عدم پیچیدگی محاسباتی، یکسان هستند. روش اول، بلوک پرچم و بخش B را در اختیار مدیر قرار می‌دهد و کنترل دو سطحی ایجاد می‌نماید و باعث افزایش امنیت می‌شود اما روش دوم این مزیت را ندارد.

در روش اول کیفیت تصویر بازیابی شده بسیار بالاتر از روش دوم است. روش دوم نسبت به روش اول دارای زحمت کم‌تری است. از مقایسه به عمل آمده در جدول۱ و اهمّیّت بعد امنیّت و وضوح تصویر روش اول نسبت به روش دوم مناسب‌تر است.

نتیجه گیری

امروزه وابستگی به کامپیوتر برای انتقال و ذخیره‌سازی اطلاعات از طریق آن افزایش یافته و به دنبال آن تهدیدات و جرایم جدیدی به وجود آمده است، از این رو نیاز به حفظ محرمانگی اطلاعات از طریق رمزنگاری احساس می‌شود. در این بین استفاده از تکنیک‌های مختلف رمزنگاری بصری و ترکیب آن با تکنیک‌های دیگر امنیّتی، محرمانگی را می‌تواند دو چندان نماید، بنابراین پیدا کردن روش مناسب با پیچیده‌گی‌های کم برای این موضوع بسیار مناسب است؛ روش رمزنگاری بصری به خاطر بار محاسباتی کم می‌تواند با دیگر تکنیک‌ها ترکیب شده و سیستم امنیّتی خوبی را ایجاد نماید.

در این مقاله بعد از بررسی چندین روش رمزنگاری بصری، دو روش رمزنگاری بصری پیشنهادی را معرفی نموده‌ایم که پس از تبدیل به تصاویر هالفتون از رمزنگاری بصری ۲ از ۲ استفاده می‌نمودند. مقایسه‌ای به این دو روش به عمل آوردیم و نتیجه حاصل برتری روش پیشنهادی اول را به روش پیشنهادی دوم از لحاظ امنیّت و وضوح تصویر اظهار داشت.

جدول۱: مقایسه و ارزیابی

روش / معیار مقایسه	روش پیشنهادی اول	روش پیشنهادی دوم
تعداد بخش‌ها	۴	۴
تعداد رمزنگاری	۳	۱
روش رمزنگاری	بصری ۲ از ۲	بصری ۲ از ۲
کنترل دو سطحی	دارد	ندارد
تصویر بازیابی شده	رنگی	سیاه و سفید
وضوح تصویر بازیابی شده	٪۷۵ تصویر اصلی	پایین
اندازه تصویر بازیابی شده	۴ برابر تصویر اصلی	۴ برابر تصویر اصلی
زحمت	بسیار	کم
امنیت	بالا- به دلیل کنترل دو سطحی	کم‌تر از روش پیشنهادی اول
پیچیدگی محاسباتی	ندارد	ندارد

منابع

1.Jaishri Chourasia, M. B. Potdar, Abdul Jhummarwala, Keyur Parmar ” Halftone Image Watermarking based on Visual Cryptography”, International Journal of Computer Applications,Vol.41,No.20, March 2012,PP.1-5.

2.Thomas Monoth , Babu Anto P ” Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes”, Procedia Computer Science, Vol.2 ,2012, PP.143-148.

3.Jenila Vincent M,E.Angeline Helena” Securing Multiple Color Secrets Using Visual Cryptography”, Procedia Engineering, Vol.38,2012,806-812.

4.Bert W. Leung, Felix Y. Ng, and Duncan S. Won ,” On the Security of a Visual Cryptography Scheme for Color Images” ,Pattern Recognition, Vol.42, No.5, May 2009,PP.929-940.

5.Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara “Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking” , IJCSI International Journal of Computer Science Issues,Vol.8,No.1,may 2011,PP.543-549.

6.Jeos J Tharayil,E.S Karthik Kumar,Neena Susan Alex”Visual Cryptography Using Hybrid Halftonig” , Procedia Engineering ,Vol.38 ,2012, PP.2117-2123.

7.Young-Chang Hou,” Visual cryptography for color images”, Pattern Recognition, Vol.36,2003,PP.1619-1629.

8.Arun Ross,Asem A.Othman, ”Visual Cryptography For Face Privacy” , Proc. of SPIE Conference on Biometric Technology for Human Identification VII , April 2010,PP.1-13.

9.Shyong Jian Shyu,Shih-Yu Huang,Yeuan-Kuen Lee, Ran-ZanWang, Kun Chen,” Sharing multiple secrets in visual cryptography”, Pattern Recognition ,Vol.40,2007,PP.3633-3651.

10.Carlo Blundo, Stelvio Cimato, Alfredo De Santis,” Visual cryptography schemes with optimal pixel expansion”, Theoretical Computer Science ,Vol.369,Desmber 2006,PP.169-182.

11.T.Rajitha, Prof P.Pradeep Kumar, V.Laxmi ”Construction of Extended Visual Cryptography Scheme for Secret Sharing”, International Journal of Computer Science and Network (IJCSN) ,Vol.1,No.4, August 2012,PP.85-90.

12.S. Cimato, R. De Prisco, A. De Santis.(2007).” Colored visual cryptography without color darkening”, Theoretical Computer Science ,Vol.374 ,2007, PP.261-276.

13.Zhi Zhou, Gonzalo R. Arce, Giovanni Di Crescenzo,” Halftone Visual Cryptography” , IEEE TRANSACTIONS ON IMAGE PROCESSING ,Vol.15,No.8, AUGUST 2006,PP.2441-2453.

14.Moni Naor,Adi Shamir “visual cryptography”, Advances in Cryptology-Eurocrypt, Vol.950,1995,PP.1-12.

15.Chang-Chou Lin, Wen-Hsiang Tsai,” Visual cryptography for gray-level images by dithering techniques”, Pattern Recognition Letters , Vol.24,2003, PP.349-358.