تایید هویت بیومتریکی بر مبنای روشهای آب نشان با استفاده از تبدیل موجک گسسته

غزاله سربیشه ئی
دانشگاه فردوسی مشهد
gh_sarbishei@yahoo.com

دکتر حسینی خیاط
دانشگاه فردوسی مشهد
saied.hosseini@gmail.com

دکتر سیدین
دانشگاه فردوسی مشهد

چکیده: در این مقاله الگوریتم مقاومی برای آب نشان گذاری در تصویر اثر انگشت به منظور بهبود عملکرد سیستمهای تایید هویت بیومتریکی ارائه شده است. در این الگوریتم از تبدیل موجک گسسته ۳ لایه و الگوریتم QSWT برای پنهان سازی داده ها استفاده شده است. داده ها در باندهای فرکانسی میانی و باند فرکانس بالا به صورت افزونه قرار می گیرند. نتایج نشان می دهند که الگوریتم ارائه شده دارای مقاومت خوبی در برابر حملات متداول بوده و بعلاوه دقت آشکار سازی نیز بسیار خوب است.

کلمات کلیدی- تبدیل موجک گسسته ، آب نشان

۱- مقدمه

امروزه بکارگیری روشهای مبتنی بر بیومتریک به منظور تایید هویت افراد بسیار مورد توجه قرار گرفته است. این روشها مزایای فراوانی نسبت به روشهای سنتی مبتنی بر امضا ، کلمات عبور و امثال آن دارند. در مقابل از چالشهای مرتبط با این گونه سیستمها می توان به تامین ایمنی آنها اشاره کرد. از جمله روشهایی که برای این منظور و به جهت مقابله با انواع حمله ها پیشنهاد شده است، استفاده از تکنیکهای آب نشان[1] می باشد.

روشهای آب نشان در تصاویر را می توان به دو دسته تقسیم بندی کرد. در دسته اول، پنهان سازی در حوزه مکان (با تغییر مقدار پیکسلها) انجام می شود. در دسته دوم ابتدا تبدیلی مانند تبدیل کسینوسی گسسته و یا تبدیل موجک گسسته[2] به تصویر اعمال شده و داده های آب نشانه در این ضرایب پنهان می شوند. تبدیل موجک گسسته تصویر را به چهار باند فرکانسی مختلف تقسیم می کند (شامل LL، LH، HL و HH). باند LL حاوی اطلاعات فرکانس پایین ، باندهای LH و HL شامل اطلاعات فرکانسهای میانی و باند HH حاوی اطلاعات فرکانس بالاست. با اعمال مجدد تبدیل موجک به باند LL ساختار چنددقتی[3] برای تبدیل ایجاد می شود. انتخاب زیر باند فرکانسی مناسب جهت پنهان سازی به عوامل مختلفی بستگی دارد، با پنهان سازی در هر یک از زیرباندهای فوق مقاومت الگوریتم در برابر دسته خاصی از حملات بهبود می یابد.

در این مقاله از تکنیک آب نشان در حوزه DWT در تصویر اثر انگشت استفاده شده است. نتایج بدست آمده نشان می دهند که الگوریتم ارائه شده در برابر حملاتی از جمله تارشدگی، فشرده سازی jpeg و افزودن نویز گوسی دارای مقاومت خوبی بوده و بعلاوه آشکارسازی آب نشانه نیز با

[1] Watermarking
[2] DWT
[3] Multiresolution Wavelet Transform

دقت مناسبی انجام می پذیرد.

در این مقاله ابتدا مروری بر سیستمهای تایید هویت بیومتریکی با استفاده از آب نشان ارائه می شود. سپس الگوریتم پیشنهادی بیان شده و نتایج شبیه سازی بررسی می شوند. در انتها نیز پیشنهادهایی در جهت بهبود عملکرد الگوریتم ارائه می شود.

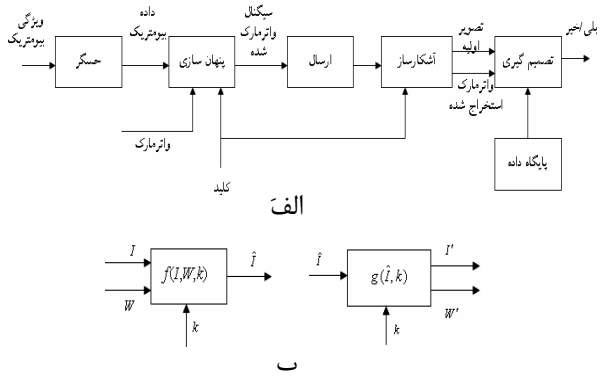
۲- سیستمهای تایید هویت بیومتریکی با استفاده از آب نشان

در یک سیستم تایید هویت مبتنی بر اثر انگشت، تصویر اثر انگشت کلیه کاربران مجاز سیستم در یک پایگاه داده ذخیره می شود. در این سیستمها به منظور افزایش سطح ایمنی سیستم و مقابله با حملات مختلف از ترکیب روشهای آب نشان با روشهای بیومتریکی استفاده می شود. ساختار یک چنین سیستمی در شکل ۱ نشان داده شده است.

برای تایید هویت کاربران بر مبنای اثر انگشت الگوریتمهای مختلفی ارائه شده است [۱ و ۲]. در برخی از این الگوریتمها، تایید هویت بر مبنای انطباق نقاط minutia اثر انگشت ورودی به سیستم با داده های موجود در پایگاه داده انجام می شود. در این مقاله minutia استخراج شده از اثر انگشت بعنوان آب نشانه در خود تصویر پنهان شده و به همراه اثر انگشت برای سیستم تایید هویت ارسال می شود. در محل گیرنده داده های آب نشانه از تصویر استخراج شده و تصویر اثر انگشت مجددا ساخته می شود. در این شرایط تایید هویت کاربران بر دو مبنا صورت می گیرد، یکی انطباق اثر انگشت بازسازی شده با تصویر موجود در پایگاه داده و دیگری آب نشانه استخراج شده. از آنجاییکه آب نشانه حاوی اطلاعات مربوط به minutia اثر انگشت (تصویر میزبان) می باشد، می توان با انطباق آنها با اطلاعات ذخیره شده در پایگاه داده، هویت کاربر را تایید نمود.

۳- الگوریتم پیشنهادی

در این مقاله از تکنیکهای مبتنی بر تبدیل DWT برای آب نشان تصویر اثر انگشت استفاده شده است. در ابتدا تبدیل DWT ۳ لایه به تصویر اعمال می شود. در اثر این عمل تصویر به ۱۰ زیر باند فرکانسی تقسیم می شود. در این الگوریتم باند LL3 که حاوی اطلاعات فرکانس پایین می باشد، بدون تغییر باقی می ماند.



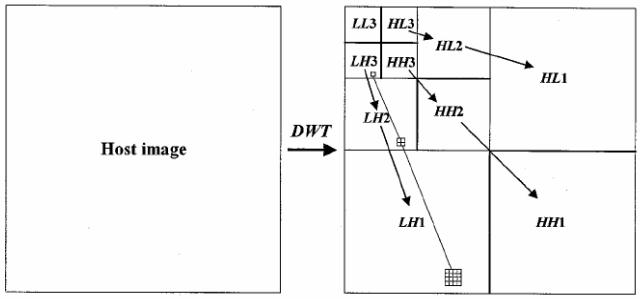
شکل ۱ الف) ساختار یک سیستم تایید هویت بیومتریکی ب) بخشهای پنهان ساز و آشکار ساز

داده آب نشانه ، شامل اطلاعات minutia، به صورت یک لیست ۳ ستونی (شامل مختصات x و y محل minutia در تصویر و گرادیان در آن محل) می باشد و مجموع این اطلاعات در ۳ باند LH، HL و HH پنهان می شوند. به منظور افزایش دقت، هر عدد آب نشانه به طور تکراری در دو لایه متوالی یکی از زیر باندهای فوق قرار می گیرد. انتخاب ضرایب مناسب جهت پنهان سازی بر مبنای روش QSWT[4] [۳] انجام می شود. در این روش بین ضرایب لایه های مختلف باندهای فرکانسی یک رابطه والد-فرزندی معرفی می شود. . در شکل ۲ نمونه ای از این رابطه نشان داده شده است.

به عبارتی با در نظر گرفتن باندهای فرکانس بالا (LH1، HL1 و HH1) می توان هر ضریب از این باند را متناظر با یک مجموعه از ضرایب لایه های بالاتر در نظر گرفت. ضریب متناظر در لایه های بالا بعنوان والد در نظر گرفته شده و ضرایب لایه های پایینتر فرزندان آنها هستند. به بیان دیگر اگر ضریب $x_n(i,j) \in D$ در باند بالا باشد که $D \subset \{LL_n, LH_n, HL_n, HH_n\}$ و $|x_n(i,j)| > T_1$ ، این ضریب والد ضریب x_{n-1} خواهد بود اگر $|x_{n-1}(i,j)| > T_2$. در این رابطه T_1 و T_2 مقادیر آستانه می باشند. در این حالت x_n و کلیه فرزندان آن تشکیل یک درخت QSWT می دهند.

به منظور پنهان سازی داده در باندهای فرکانس میانی، پس از اعمال DWT ۳ لایه با اجرای روش QSWT، ضرایب مناسب در باندهای LH2، LH3 ، HL2، HL3 ، HH2 و HH3

[4] Qualified significant wavelet tree



شکل ۲ تبدیل موجک چند لایه. فلشها از باندهای والد به سمت باندهای فرزند هستند [۳]

را انتخاب می کنیم که مقدار آستانه مناسب برای هر یک از این باندها طبق رابطه زیر تعیین می شود:

$$T_3 = \{\bar{x}_3 \mid x_1,...,x_n \in LH3 or HL3 or HH3\} \quad (۱)$$

$$T_2 = \{\bar{x}_2 \mid x_1,...,x_n \in LH2 or HL2 or HH2\} \quad (۲)$$

جهت پنهان سازی دادها نیز ابتدا اطلاعات minutia به یک رشته عدد تبدیل می شوند. از آنجاییکه تعداد ضرایب والد بدست آمده به روش QSWT در باندهای LH3 ، HL3 و HH3 با یکدیگر متفاوت است، رشته اعداد بدست آمده به ۳ رشته آب نشانه با طولهای متفاوت تقسیم می شوند. اعداد هر یک از این رشته ها نیز در ضرایب والد و یکی از ضرایب فرزندان در لایه های پایین بر طبق رابطه زیر پنهان می شوند.

$$x'_3(i,j) = x_3(i,j) + \alpha w_l(k) \quad (۳)$$

$$x'_2(i,j) = x_2(i,j) + \alpha w_l(k) \quad (۴)$$

که در این روابط x_3 ضرایب والد در یکی از باندهای LH ، HL و HH بوده و x_2 نیز ضریب یکی از فرزند متناظر آن است که بزرگترین مقدار را دارد. x'_3 و x'_3 ضرایب مربوط به تصویر آب نشان دار و w_l نیز مقدار آب نشانه می باشد. α پارامتری است که قدرت پنهان سازی را نشان می دهد. هر چه این پارامتر بزرگتر باشد، تغییرات ایجاد شده در کیفیت تصویر محسوس تر خواهد بود. پس از پنهان سازی کلیه اعداد در ضرایب DWT ، تبدیل IDWT[5] اعمال شده و تصویر آب نشان دار ساخته می شود.

به منظور آشکارسازی و استخراج اعداد آب نشانه، پس از اعمال تبدیل DWT به دو تصویر اصلی (موجود در پایگاه داده) و تصویر آب نشان دار، طبق رابطه زیر مقدار آب نشانه استخراج می شود:

$$Y = DWT(X) \quad (۵)$$

$$Y' = DWT(X')$$

$$\begin{cases} W_i^3 = Y'_{i(LH3)} - Y_{h(LH3)} \\ W_i^2 = Y'_{i(LH2)} - Y_{h(LH2)} \end{cases} \Rightarrow \quad \hat{W}_i = 1/2\alpha\,(W_i^3 + W_i^2) \quad (۶)$$

برای کلیه ضرایب.

به منظور تامین اهداف ایمنی، لازم است از یک کلید سری استفاده شود. برای این منظور، استخراج ۳ رشته از آب نشانه اولیه بر اساس یک رشته شبه تصادفی انجام می شود و هسته لازم برای تولید این رشته، همان کلمه عبوری انتخاب می شود که سیستم در اختیار هر کاربر قرار داده است.

۴- بررسی نتایج شبیه سازی

الگوریتم فوق بر روی یک پایگاه داده شامل ۱۰۰ تصویر اثر انگشت شبیه سازی و اجرا شده است و عملکرد آن در برابر

نویز گوسی، تار شدگی، sharpening، Median filtering ، فشرده سازی jpeg و تصحیحات گاما بررسی شده است. در شکل ۳ نمونه ای از یک تصویر اثر انگشت قبل و بعد از پنهان سازی نشان داده شده است. برای بررسی کیفیت سیگنال میزبان قبل و بعد از پنهان سازی معیار PSNR[6] به صورت زیر تعریف می شود:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - \hat{I}(x,y)\right)^2 \quad (۷)$$

$$PSNR = 10\log\frac{255^2}{MSE} \quad (۸)$$

در این روابط M و N سایز تصاویر و $I(x,y)$ و $\hat{I}(x,y)$ به ترتیب مقادیر تصویر میزبان و تصویر آب نشان دار می باشند.

[5] Inverse Discrete Wavelet Transform

[6] Peak Signal to Noise Ratio

ب الف

شکل ۳ الف)اثر انگشت اولیه ب) اثر انگشت با آبنشان

جدول ۱ نتایج شبیه سازی برای حملات مختلف

	PSNR	Correlation	Error Rate
No attack	85.96	1	0
Gaussian Noise	83.57	0.9992	0
Blurring	74.41	0.899	6.6%
Sharpening	57.839	0.7482	20.7%
Median filtering	76.91	.9358	1.48%
JPEG Compression	80.37	0.9507	1.44%
Gamma Correction	86.85	0.9584	0.86%

همچنین میزان شباهت آب نشانه استخراج شده با معیار همبستگی سنجیده می شود:

$$\rho = \frac{\sum (x-\bar{x})(y-\bar{y})}{\sqrt{\sum (x-\bar{x})^2}\sqrt{\sum (y-\bar{y})^2}} \qquad (۹)$$

که در این رابطه x و y به ترتیب معرف آب نشانه اولیه و مقدار استخراج شده از تصویر می باشند.

نرخ خطای آشکار سازی نیز در هر یک از موارد محاسبه شده است. این نتایج در جدول ۱ آورده شده است. همانگونه که مشاهده می شود الگوریتم دارای مقاومت نسبتا خوبی در برابر حملات متداول ، به ویژه نویز گوسی و فشرده سازی jpeg دارد.

از پارامترهای مهم دیگری نیز که در عملکرد سیستمهای آب نشان حائز اهمیت است، ظرفیت پنهان سازی می باشد. در این الگوریتم ظرفیت به صورت مقدار اطلاعاتی بیان می شود که می توان در یک تصویر پنهان نمود. در الگوریتم ارائه شده، بطور متوسط تصاویر با ابعاد ۴۲۰×۴۳۰ قابلیت پنهان سازی ۱۴۱ عدد آب نشانه را دارند.

نکته مهم دیگری که لازم است مد نظر قرار گیرد، عملکرد سیستم تایید هویت کاربر پس از استخراج آب نشانه در تصویر اثر انگشت است. در این مقاله نتایج عملکرد سیستم تایید هویت [۴] نشان دهنده عدم تغییر عملکرد سیستم تایید هویت پس از استخراج آب نشانه می باشد.

۵ - نتیجه گیری

در این مقاله الگوریتمی معرفی شد که با استفاده از تبدیل موجک ۳ لایه برای آب نشان تصویر اثر انگشت منجر به مقاومت خوبی در برابر حملات متداول شده است.داده های آب نشانه minutia استخراج شده از تصویر اثر انگشت می باشد که در گیرنده با استخراج این داده ها هویت کاربر تصدیق می شود. نتایج نشان می دهد که فرایند پنهان سازی با وجود حملات مختلف تاثیری در عملکرد سیستم تایید هویت بر مبنای اثر انگشت نخواهد داشت.

مراجع

[1] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, "An identity-authentication system using fingerprints", *Proceeding IEEE*, vol.85, no.9 SEP. 1997.

[2] A. K. Jain, L. Hong, R. Bolle, "On-line fingerprint verification", *IEEE Trans. Pattern analysis And Machine intelligence*, Vol.19, no.4, 1997.

[3] M. Hsieh, D. Tseng, Y. Huangm "Hiding digital watermarks using multiresolution wavelet transform", *IEEE Trans. Industrial Electronics*, vol. 48, no.5, oct. 2001.

[4] http://www.neurotechnologija.com/